Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
Application					
Ablgenesistoken Project					
Ablgenesistoken					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for ABLGenesisToken, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13741**	https://github.com/BlockChainsSecurity/EtherTokens/tree/master/ABLGenesisToken, https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md	**A-Abl-Ablge/01-08-18/1**
Anovabace Project					
Anovabace					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for AnovaBace, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13737**	https://github.com/BlockChainsSecurity/EtherTokens/tree/master/AnovaBace, https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md	**A-Ano-Anova/01-08-18/2**
Appletoken Project					
Appletoken					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for AppleToken, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of	https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overf	**A-App-Apple/01-08-18/3**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			an arbitrary user to any value. **CVE-ID:CVE-2018-13776**	low.md, https://github.com/BlockChainsSecurity/EtherTokens/tree/master/AppleToken	
Azttoken Project					
Azttoken					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for AZTToken, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13734**	https://github.com/BlockChainsSecurity/EtherTokens/tree/master/AZTToken, https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md	**A-Azt-Aztto/01-08-18/4**
Bcaas Project					
Bcaas					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for BCaaS, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13665**	https://github.com/BlockChainsSecurity/EtherTokens/tree/master/BCaaS, https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md	**A-Bca-Bcaas/01-08-18/5**
Bigcadvancedtoken Project					
Bigcadvancedtoken					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for BIGCAdvancedToken, an Ethereum token, has an integer	https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GE	**A-Big-Bigca/01-08-18/6**

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13759**	MCHAIN/mint%20integer%20overflow.md, https://github.com/BlockChainsSecurity/EtherTokens/tree/master/BIGCAdvancedToken	
Biqutoken Project					
Biqutoken					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for BiquToken, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13764**	https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md, https://github.com/BlockChainsSecurity/EtherTokens/tree/master/BiquToken	**A-Biq-Biqut/01-08-18/7**
Bitedutoken Project					
Bitedutoken					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for BiteduToken, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13719**	https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md, https://github.com/BlockChainsSecurity/EtherTokens/tree/master/BiteduToken	**A-Bit-Bited/01-08-18/8**
Bitstarti Project					
Bitstarti					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation	https://github.com/BlockChainsSec	**A-Bit-Bitst/01-**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			for Bitstarti, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13774**	urity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md, https://github.com/BlockChainsSecurity/EtherTokens/tree/master/Bitstarti	**08-18/9**
Bpstoken Project					
Bpstoken					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for BpsToken, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13715**	https://github.com/BlockChainsSecurity/EtherTokens/tree/master/BpsToken, https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md	**A-Bps-Bpsto/01-08-18/10**
Bsctoken Project					
Bsctoken					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for BSCToken, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13663**	https://github.com/BlockChainsSecurity/EtherTokens/tree/master/BSCToken, https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md	**A-Bsc-Bscto/01-08-18/11**
Btpcoin Project					
Btpcoin					

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for BTPCoin, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13668**	https://github.com/BlockChainsSecurity/EtherTokens/tree/master/BTPCoin, https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md	**A-Btp-Btpco/01-08-18/12**
Buytoken Project					
Buytoken					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for Order (ETH) (Contract Name: BuyToken), an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13708**	https://github.com/BlockChainsSecurity/EtherTokens/tree/master/BuyToken, https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md	**A-Buy-Buyto/01-08-18/13**
Cartoken Project					
Cartoken					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for CarToken, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13748**	https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md, https://github.com/BlockChainsSecurity/EtherTokens/tree/master/CarToken	**A-Car-Carto/01-08-18/14**
Cerb Coin Project					

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
Cerb Coin					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for CERB_Coin, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13703**	https://github.com/BlockChainsSecurity/EtherTokens/tree/master/CERB_Coin, https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md	**A-Cer-Cerb/01-08-18/15**
Cgctoken Project					
Cgctoken					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for CGCToken, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13778**	https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md, https://github.com/BlockChainsSecurity/EtherTokens/tree/master/CGCToken	**A-Cgc-Cgcto/01-08-18/16**
Cherrycoinfoundation Project					
Cherrycoinfoundation					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for CherryCoinFoundation, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13756**	https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md, https://github.com/BlockChainsSecurity/EtherTokens/tree/master/CherryCoinFoundation	**A-Che-Cherr/01-08-18/17**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
Cjxtoken Project					
Cjxtoken					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for CJXToken, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13689**	https://github.com/BlockChainsSecurity/EtherTokens/tree/master/CJXToken, https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md	**A-Cjx-Cjxto/01-08-18/18**
Cm Project					
CM					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for CM, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13714**	https://github.com/BlockChainsSecurity/EtherTokens/tree/master/CM, https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md	**A-Cm-CM/01-08-18/19**
Coinquer Project					
Coinquer					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for Coinquer, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13757**	https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md, https://github.com/BlockChainsSecurity/EtherTokens/tree/master/Coinquer	**A-Coi-Coinq/01-08-18/20**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
Combilladvancedtoken Project					
Combilladvancedtoken					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for ComBillAdvancedToken, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13674**	https://github.com/BlockChainsSecurity/EtherTokens/tree/master/ComBillAdvancedToken, https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md	**A-Com-Combi/01-08-18/21**
Cornerstone Project					
Cornerstone					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for Cornerstone, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13767**	https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md, https://github.com/BlockChainsSecurity/EtherTokens/tree/master/Cornerstone	**A-Cor-Corne/01-08-18/22**
Crowdnext Project					
Crowdnext					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for Crowdnext (CNX), an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13744**	https://github.com/BlockChainsSecurity/EtherTokens/tree/master/Crowdnext, https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GE	**A-Cro-Crowd/01-08-18/23**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
				MCHAIN/mint%20integer%20overflow.md	
Cryptosistoken Project					
Cryptosistoken					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for CryptosisToken, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13754**	https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md, https://github.com/BlockChainsSecurity/EtherTokens/tree/master/CryptosisToken	**A-Cry-Crypt/01-08-18/24**
Ctest7 Project					
Ctest7					
Overflow	09-07-2018	**5**	The mint function of a smart contract implementation for CTest7, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13695**	https://github.com/BlockChainsSecurity/EtherTokens/tree/master/CTest7, https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md	**A-Cte-Ctest/01-08-18/25**
Cws Project					
CWS					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for CWS, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13664**	https://github.com/BlockChainsSecurity/EtherTokens/tree/master/CWS, https://github.com/BlockChainsSec	**A-Cws-CWS/01-08-18/26**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
				urity/EtherTokens /blob/master/GE MCHAIN/mint%2 0integer%20overf low.md	
Databits Project					
Databits					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for Databits, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13711**	https://github.co m/BlockChainsSec urity/EtherTokens /tree/master/Dat abits, https://github.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 0integer%20overf low.md	**A-Dat-Datab/01 -08-18/27**
Destineed Project					
Destineed					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for DestiNeed (DSN), an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13699**	https://github.co m/BlockChainsSec urity/EtherTokens /tree/master/Des tiNeedToken, https://github.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 0integer%20overf low.md	**A-Des-Desti/01-08-18/28**
Deweisecurityservicetoken Project					
Deweisecurityservicetoken					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for DeWeiSecurityServiceToken, an Ethereum token, has an integer overflow that allows	https://github.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 0integer%20overf	**A-Dew-Dewei/01 -08-18/29**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13753**	low.md, https://github.com/BlockChainsSecurity/EtherTokens/tree/master/DeWeiSecurityServiceToken	
Dinsteincoin Project					
Dinsteincoin					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for DinsteinCoin, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13671**	https://github.com/BlockChainsSecurity/EtherTokens/tree/master/DinsteinCoin, https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md	**A-Din-Dinst/01-08-18/30**
Dopnetwork Project					
Dopnetwork					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for dopnetwork, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13739**	https://github.com/BlockChainsSecurity/EtherTokens/tree/master/dopnetwork, https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md	**A-Dop-Dopne/01-08-18/31**
Eastcoin Project					
Eastcoin					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for Eastcoin, an Ethereum	https://github.com/BlockChainsSecurity/EtherTokens	**A-Eas-Eastc/01-08-18/32**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13727**	/blob/master/GEMCHAIN/mint%20integer%20overflow.md, https://github.com/BlockChainsSecurity/EtherTokens/tree/master/Eastcoin	
Easticoin Project					
Easticoin					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for Easticoin, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13766**	https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md, https://github.com/BlockChainsSecurity/EtherTokens/tree/master/Easticoin	**A-Eas-Easti/01-08-18/33**
Eddtoken Project					
Eddtoken					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for eddToken, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13704**	https://github.com/BlockChainsSecurity/EtherTokens/tree/master/eddToken, https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md	**A-Edd-Eddto/01-08-18/34**
Elearningcoinerc Project					
Elearningcoinerc					
Overflow	09-07-2018	**5**	The mintToken function of a	https://github.co	**A-Ele-**

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			smart contract implementation for ELearningCoinERC, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13736**	m/BlockChainsSecurity/EtherTokens/tree/master/ELearningCoinERC, https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md	**Elear/01-08-18/35**
Entercoin Project					
Entercoin					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for ENTER (ENTR) (Contract Name: EnterCoin), an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13782**	https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md, https://github.com/BlockChainsSecurity/EtherTokens/tree/master/EnterCoin	**A-Ent-Enter/01-08-18/36**
Entertoken Project					
Entertoken					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for ENTER (ENTR) (Contract Name: EnterToken), an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13735**	https://github.com/BlockChainsSecurity/EtherTokens/tree/master/EnterToken, https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md	**A-Ent-Enter/01-08-18/37**
Eristicaico Project					

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
Eristicaico					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for EristicaICO, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13666**	https://github.com/BlockChainsSecurity/EtherTokens/tree/master/EristicaICO, https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md	**A-Eri-Erist/01-08-18/38**
Esh Project					
ESH					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for ESH, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13780**	https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md, https://github.com/BlockChainsSecurity/EtherTokens/tree/master/ESH	**A-Esh-ESH/01-08-18/39**
Essence Project					
Essence					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for Essence, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13702**	https://github.com/BlockChainsSecurity/EtherTokens/tree/master/Essence, https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md	**A-Ess-Essen/01-08-18/40**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
Exacorecontract Project					
Exacorecontract					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for ExacoreContract, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13771**	https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md, https://github.com/BlockChainsSecurity/EtherTokens/tree/master/ExacoreContract	**A-Exa-Exaco/01-08-18/41**
Exsulcoin Project					
Exsulcoin					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for exsulcoin, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13683**	https://github.com/BlockChainsSecurity/EtherTokens/tree/master/exsulcoin, https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md	**A-Exs-Exsul/01-08-18/42**
Ffmpeg					
Ffmpeg					
DoS	05-07-2018	**4.3**	In FFmpeg 4.0.1, a missing check for failure of a call to init_get_bits8() in the avpriac3_parse_header function in libavcodec/ac3_parser.c may trigger a NULL pointer dereference while converting a crafted AVI file to MPEG4, leading to a denial of service. CVE-ID:CVE-2018-13303	https://github.com/FFmpeg/FFmpeg/commit/00e8181bd97c834fe60751b0c511d4bb97875f78	**A-Ffm-Ffmpe/01-08-18/43**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
DoS	05-07-2018	**4.3**	In FFmpeg 4.0.1, due to a missing check of a profile value before setting it, the ff_mpeg4_decode_picture_header function in libavcodec/mpeg4videodec.c may trigger a NULL pointer dereference while converting a crafted AVI file to MPEG4, leading to a denial of service. **CVE-ID:CVE-2018-13301**	https://github.com/FFmpeg/FFmpeg/commit/2aa9047486dbff12d9e040f917e5f799ed2fd78b	**A-Ffm-Ffmpe/01-08-18/44**
DoS	05-07-2018	**4.3**	In libavcodec in FFmpeg 4.0.1, improper maintenance of the consistency between the context profile field and studio_profile in libavcodec may trigger an assertion failure while converting a crafted AVI file to MPEG4, leading to a denial of service, related to error_resilience.c, h263dec.c, and mpeg4videodec.c. **CVE-ID:CVE-2018-13304**	https://github.com/FFmpeg/FFmpeg/commit/bd27a9364ca274ca97f1df6d984e88a0700fb235	**A-Ffm-Ffmpe/01-08-18/45**
DoS	05-07-2018	**5.8**	In FFmpeg 4.0.1, an improper argument (AVCodecParameters) passed to the avprirequest_sample function in the handle_eac3 function in libavformat/movenc.c may trigger an out-of-array read while converting a crafted AVI file to MPEG4, leading to a denial of service and possibly an information disclosure. **CVE-ID:CVE-2018-13300**	https://www.debian.org/security/2018/dsa-4249, https://github.com/FFmpeg/FFmpeg/commit/95556e27e2c1d56d9e18f5db34d6f756f3011148	**A-Ffm-Ffmpe/01-08-18/46**
DoS	05-07-2018	**5.8**	In FFmpeg 4.0.1, due to a missing check for negative values of the mquant variable, the vc1_put_blocks_clamped function in libavcodec/vc1_block.c may trigger an out-of-array access	https://github.com/FFmpeg/FFmpeg/commit/d08d4a8c7387e758d439b0592782e4cfa2b4d6a4	**A-Ffm-Ffmpe/01-08-18/47**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			while converting a crafted AVI file to MPEG4, leading to an information disclosure or a denial of service. **CVE-ID:CVE-2018-13305**		
DoS	05-07-2018	**6.8**	In FFmpeg 4.0.1, improper handling of frame types (other than EAC3_FRAME_TYPE_INDEPENDENT) that have multiple independent substreams in the handle_eac3 function in libavformat/movenc.c may trigger an out-of-array access while converting a crafted AVI file to MPEG4, leading to a denial of service or possibly unspecified other impact. **CVE-ID:CVE-2018-13302**	https://www.debian.org/security/2018/dsa-4249, https://github.com/FFmpeg/FFmpeg/commit/ed22dc22216f74c75ee7901f82649e1ff725ba50	**A-Ffm-Ffmpe/01-08-18/48**
Finaltoken Project					
Finaltoken					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for FinalToken, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13749**	https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md, https://github.com/BlockChainsSecurity/EtherTokens/tree/master/FinalToken	**A-Fin-Final/01-08-18/49**
Futurxe Project					
Futurxe					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for FuturXe, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13718**	https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md,	**A-Fut-Futur/01-08-18/50**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
				https://github.com/BlockChainsSecurity/EtherTokens/tree/master/FuturXe	
Gfcb Project					
Gfcb					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for GFCB, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13670**	https://github.com/BlockChainsSecurity/EtherTokens/tree/master/GFCB, https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md	**A-Gfc-Gfcb/01-08-18/51**
Globalsupergametoken Project					
Globalsupergametoken					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for GlobalSuperGameToken, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13725**	https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md, https://github.com/BlockChainsSecurity/EtherTokens/tree/master/GlobalSuperGameToken	**A-Glo-Globa/01-08-18/52**
Globecoin Project					
Globecoin					
Overflow	12-07-2018	**5**	An integer overflow vulnerability exists in the function transfer_tokens_after_ICO of GlobeCoin (GLB), an Ethereum	https://github.com/VenusADLab/EtherTokens/tree/master/GlobeCoin%28GLB%29,	**A-Glo-Globe/01-08-18/53**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			token smart contract. An attacker could use it to set any user's balance. **CVE-ID:CVE-2018-14004**	https://github.com/VenusADLab/EtherTokens/blob/master/SHARKTECH/SHARKTECH.md	
Gmile Project					
Gmile					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for GMile, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13694**	https://github.com/BlockChainsSecurity/EtherTokens/tree/master/GMile, https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md	**A-Gmi-Gmile/01-08-18/54**
Goldtokenerc20 Project					
Goldtokenerc20					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for GoldTokenERC20, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13673**	https://github.com/BlockChainsSecurity/EtherTokens/tree/master/GoldTokenERC20, https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md	**A-Gol-Goldt/01-08-18/55**
Gomineworld Project					
Gomineworld					

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for GoMineWorld, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13721**	https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md, https://github.com/BlockChainsSecurity/EtherTokens/tree/master/GoMineWorld	**A-Gom-Gomin/01-08-18/56**
Goochain Project					
Goochain					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for Goochain, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13677**	https://github.com/BlockChainsSecurity/EtherTokens/tree/master/Goochain, https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md	**A-Goo-Gooch/01-08-18/57**
Greenenergytoken Project					
Greenenergytoken					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for GreenEnergyToken, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13693**	https://github.com/BlockChainsSecurity/EtherTokens/tree/master/GreenEnergyToken, https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md	**A-Gre-Green/01-08-18/58**
Hey Project					

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
HEY					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for HEY, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13730**	https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md, https://github.com/BlockChainsSecurity/EtherTokens/tree/master/HEY	**A-Hey-HEY/01-08-18/59**
Hormitechtoken Project					
Hormitechtoken					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for HormitechToken, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13717**	https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md, https://github.com/BlockChainsSecurity/EtherTokens/tree/master/HormitechToken	**A-Hor-Hormi/01-08-18/60**
Hyipcrowdsale1 Project					
Hyipcrowdsale1					
Overflow	09-07-2018	**5**	The mint function of a smart contract implementation for HYIPCrowdsale1, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13724**	https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md, https://github.com/BlockChainsSecurity/EtherTokens/tree/master/HYIPCrowdsale1	**A-Hyi-Hyipc/01-08-18/61**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
Hyiptoken Project					
Hyiptoken					
Overflow	09-07-2018	**5**	The mint function of a smart contract implementation for HYIPToken, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13722**	https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md, https://github.com/BlockChainsSecurity/EtherTokens/tree/master/HYIPToken	**A-Hyi-Hyipt/01-08-18/62**
Ico Dollar Project					
Ico Dollar					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for ICO Dollar (ICOD), an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13686**	https://github.com/BlockChainsSecurity/EtherTokens/tree/master/ICODollar, https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md	**A-Ico-Ico/01-08-18/63**
Ideacoin Project					
Ideacoin					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for IdeaCoin, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13706**	https://github.com/BlockChainsSecurity/EtherTokens/tree/master/IdeaCoin,https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md	**A-Ide-Ideac/01-08-18/64**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
Instacocoa Project					
Instacocoa					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for Instacocoa, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13690**	https://github.com/BlockChainsSecurity/EtherTokens/tree/master/Instacocoa, https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md	**A-Ins-Insta/01-08-18/65**
Ipmcoin Project					
Ipmcoin					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for IPMCoin, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13700**	https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md, https://github.com/BlockChainsSecurity/EtherTokens/tree/master/IPMCoin	**A-Ipm-Ipmco/01-08-18/66**
Iseevoicetoken Project					
Iseevoicetoken					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for ISeeVoiceToken, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13726**	https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md, https://github.com/BlockChainsSecurity/EtherTokens	**A-Ise-Iseev/01-08-18/67**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
				/tree/master/ISeeVoiceToken	
Jeanstoken Project					
Jeanstoken					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for JeansToken, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13769**	https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md, https://github.com/BlockChainsSecurity/EtherTokens/tree/master/JeansToken	**A-Jea-Jeans/01-08-18/68**
Jiucaitoken Project					
Jiucaitoken					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for JiucaiToken, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13783**	https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md, https://github.com/BlockChainsSecurity/EtherTokens/tree/master/JiucaiToken	**A-Jiu-Jiuca/01-08-18/69**
Jixocoin Project					
Jixocoin					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for JixoCoin, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13728**	https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md, https://github.co	**A-Jix-Jixoc/01-08-18/70**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
				m/BlockChainsSecurity/EtherTokens/tree/master/JixoCoin	
Jpmd100b Project					
Jpmd100b					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for JPMD100B, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13729**	https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md, https://github.com/BlockChainsSecurity/EtherTokens/tree/master/JPMD100B	**A-Jpm-Jpmd1/01-08-18/71**
Justwallet Project					
Justwallet					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for JustWallet, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13751**	https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md, https://github.com/BlockChainsSecurity/EtherTokens/tree/master/JustWallet	**A-Jus-Justw/01-08-18/72**
Kbit Project					
Kbit					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for kBit, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value.	https://github.com/BlockChainsSecurity/EtherTokens/tree/master/kBit, https://github.com/BlockChainsSec	**A-Kbi-Kbit/01-08-18/73**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			CVE-ID:CVE-2018-13746	urity/EtherTokens /blob/master/GE MCHAIN/mint%2 0integer%20overf low.md	
Kissme Project					
Kissme					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for KissMe, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13701**	https://github.co m/BlockChainsSec urity/EtherTokens /tree/master/Kiss Me, https://github.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 0integer%20overf low.md	**A-Kis-Kissm/01 -08-18/74**
Landcoin Project					
Landcoin					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for Antoken, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13720**	https://github.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 0integer%20overf low.md, https://github.co m/BlockChainsSec urity/EtherTokens /tree/master/Ant oken	**A-Lan-Landc/01 -08-18/75**
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for LandCoin, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13765**	https://github.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 0integer%20overf low.md, https://github.co	**A-Lan-Landc/01 -08-18/76**

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
				m/BlockChainsSecurity/EtherTokens/tree/master/LandCoin	
Lexittoken Project					
Lexittoken					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for LexitToken, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13680**	https://github.com/BlockChainsSecurity/EtherTokens/tree/master/LexitToken, https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md	**A-Lex-Lexit/01-08-18/77**
Lolicoin Project					
Lolicoin					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for LoliCoin, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13758**	https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md, https://github.com/BlockChainsSecurity/EtherTokens/tree/master/LoliCoin	**A-Lol-Lolic/01-08-18/78**
Lottery Project					
Lottery					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for Lottery, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value.	https://github.com/BlockChainsSecurity/EtherTokens/tree/master/Lottery, https://github.co	**A-Lot-Lotte/01-08-18/79**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			CVE-ID:CVE-2018-13678	m/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md	
Malaysia Coins Project					
Malaysia Coins					
Overflow	12-07-2018	**5**	An integer overflow vulnerability exists in the function transferAny of Malaysia coins (Xmc), an Ethereum token smart contract. An attacker could use it to set any user's balance. **CVE-ID:CVE-2018-14005**	https://github.com/VenusADLab/EtherTokens/tree/master/Malaysia%20coins%28Xmc%29, https://github.com/VenusADLab/EtherTokens/blob/master/SHARKTECH/SHARKTECH.md	**A-Mal-Malay/01-08-18/80**
Malltoken Project					
Malltoken					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for MallToken, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13688**	https://github.com/BlockChainsSecurity/EtherTokens/tree/master/MallToken, https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md	**A-Mal-Mallt/01-08-18/81**
Mehditazitoken Project					
Mehditazitoken					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for MehdiTAZIToken, an Ethereum token, has an integer overflow that allows the owner	https://github.com/BlockChainsSecurity/EtherTokens/tree/master/MehdiTAZIToken,	**A-Meh-Mehdi/01-08-18/82**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13692**	https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md	
Mjolnir Project					
Mjolnir					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for Mjolnir, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13710**	https://github.com/BlockChainsSecurity/EtherTokens/tree/master/Mjolnir, https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md	**A-Mjo-Mjoln/01-08-18/83**
Moneychainnet Project					
Moneychainnet					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for MoneyChainNet (MCN), an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13760**	https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md, https://github.com/BlockChainsSecurity/EtherTokens/tree/master/MoneyChainNetToken	**A-Mon-Money/01-08-18/84**
Mp3 Coin Project					
Mp3 Coin					
Overflow	12-07-2018	**5**	An integer overflow vulnerability exists in the function distribute of MP3	https://github.com/VenusADLab/EtherTokens/tree/	**A-Mp3-Mp3/01-08-18/85**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			Coin (MP3), an Ethereum token smart contract. An attacker could use it to set any user's balance. **CVE-ID:CVE-2018-14002**	master/MP3%20Coin%28MP3%29, https://github.com/VenusADLab/EtherTokens/blob/master/SHARKTECH/SHARKTECH.md	
Myylc Project					
Myylc					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for MyYLC, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13781**	https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md, https://github.com/BlockChainsSecurity/EtherTokens/tree/master/MyYLCToken	**A-Myy-Myylc/01-08-18/86**
Ncu Project					
NCU					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for NCU, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13669**	https://github.com/BlockChainsSecurity/EtherTokens/tree/master/NCU, https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md	**A-Ncu-NCU/01-08-18/87**
Neo Genesis Token Project					
Neo Genesis Token					

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
Overflow	12-07-2018	**5**	An integer overflow vulnerability exists in the function multipleTransfer of Neo Genesis Token (NGT), an Ethereum token smart contract. An attacker could use it to set any user's balance. **CVE-ID:CVE-2018-14006**	https://github.com/VenusADLab/EtherTokens/tree/master/Neo%20Genesis%20Token%28NGT%29, https://github.com/VenusADLab/EtherTokens/blob/master/SHARKTECH/SHARKTECH.md	**A-Neo-Neo/01-08-18/88**
Netkilleradvancedtokenairdrop Project					
Netkilleradvancedtokenairdrop					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for NetkillerAdvancedTokenAirDrop, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13761**	https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md, https://github.com/BlockChainsSecurity/EtherTokens/tree/master/NetkillerAdvancedTokenAirDrop	**A-Net-Netki/01-08-18/89**
Netkillertoken Project					
Netkillertoken					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for Enterprise Token Ecosystem (ETE) (Contract Name: NetkillerToken), an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13773**	https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md, https://github.com/BlockChainsSecurity/EtherTokens/tree/master/NetkillerToken	**A-Net-Netki/01-08-18/90**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
Normikaivo Project					
Normikaivo					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for normikaivo, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13687**	https://github.com/BlockChainsSecurity/EtherTokens/tree/master/normikaivo, https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md	**A-Nor-Normi/01-08-18/91**
Obtcoin Project					
Obtcoin					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for OBTCoin, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13672**	https://github.com/BlockChainsSecurity/EtherTokens/tree/master/OBTCoin, https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md	**A-Obt-Obtco/01-08-18/92**
Onechain Project					
Onechain					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for OneChain, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13740**	https://github.com/BlockChainsSecurity/EtherTokens/tree/master/OneChain, https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%2	**A-One-Onech/01-08-18/93**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
				0integer%20overflow.md	
Oracle					
Agile Product Lifecycle Management For Process					
NA	18-07-2018	**4**	Vulnerability in the Oracle Agile Product Lifecycle Management for Process component of Oracle Supply Chain Products Suite (subcomponent: Installation). The supported version that is affected is 6.2.0.0. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Agile Product Lifecycle Management for Process. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Agile Product Lifecycle Management for Process accessible data. CVSS 3.0 Base Score 2.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N). **CVE-ID:CVE-2018-3069**	NA	**A-Ora-Agile/01-08-18/94**
Applications Manager					
NA	18-07-2018	**5**	Vulnerability in the Oracle Applications Manager component of Oracle E-Business Suite (subcomponent: Oracle Diagnostics Interfaces). Supported versions that are affected are 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6 and 12.2.7. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle	NA	**A-Ora-Appli/01-08-18/95**

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			Applications Manager. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Applications Manager accessible data. CVSS 3.0 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE-ID:CVE-2018-2996**		
Banking Corporate Lending					
DoS	18-07-2018	**5.5**	Vulnerability in the Oracle Banking Corporate Lending component of Oracle Financial Services Applications (subcomponent: Core module). Supported versions that are affected are 12.3.0, 12.4.0, 12.5.0, 14.0.0 and 14.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Banking Corporate Lending. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Banking Corporate Lending accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Banking Corporate Lending. CVSS 3.0 Base Score 5.4 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:L). **CVE-ID:CVE-2018-3042**	NA	**A-Ora-Banki/01-08-18/96**
DoS	18-07-2018	**6.5**	Vulnerability in the Oracle Banking Corporate Lending component of Oracle Financial	NA	**A-Ora-Banki/01-08-18/97**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			Services Applications (subcomponent: Core module). Supported versions that are affected are 12.3.0, 12.4.0, 12.5.0, 14.0.0 and 14.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Banking Corporate Lending. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Banking Corporate Lending accessible data as well as unauthorized read access to a subset of Oracle Banking Corporate Lending accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Banking Corporate Lending. CVSS 3.0 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L). **CVE-ID:CVE-2018-3036**		
NA	18-07-2018	**3.5**	Vulnerability in the Oracle Banking Corporate Lending component of Oracle Financial Services Applications (subcomponent: Core module). Supported versions that are affected are 12.3.0, 12.4.0, 12.5.0, 14.0.0 and 14.1.0. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Banking Corporate Lending. Successful attacks of this vulnerability can	NA	**A-Ora-Banki/01-08-18/98**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			result in unauthorized access to critical data or complete access to all Oracle Banking Corporate Lending accessible data. CVSS 3.0 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N). **CVE-ID:CVE-2018-3046**		
NA	18-07-2018	**4**	Vulnerability in the Oracle Banking Corporate Lending component of Oracle Financial Services Applications (subcomponent: Core module). Supported versions that are affected are 12.3.0, 12.4.0, 12.5.0, 14.0.0 and 14.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Banking Corporate Lending. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Banking Corporate Lending. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). **CVE-ID:CVE-2018-3040**	NA	**A-Ora-Banki/01-08-18/99**
NA	18-07-2018	**4.9**	Vulnerability in the Oracle Banking Corporate Lending component of Oracle Financial Services Applications (subcomponent: Core module). Supported versions that are affected are 12.3.0, 12.4.0, 12.5.0, 14.0.0 and 14.1.0. Easily exploitable vulnerability allows low privileged attacker	NA	**A-Ora-Banki/01-08-18/100**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			with network access via HTTP to compromise Oracle Banking Corporate Lending. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Banking Corporate Lending, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Banking Corporate Lending accessible data as well as unauthorized read access to a subset of Oracle Banking Corporate Lending accessible data. CVSS 3.0 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N). **CVE-ID:CVE-2018-3048**		
NA	18-07-2018	**5**	Vulnerability in the Oracle Banking Corporate Lending component of Oracle Financial Services Applications (subcomponent: Core module). Supported versions that are affected are 12.3.0, 12.4.0, 12.5.0, 14.0.0 and 14.1.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Banking Corporate Lending. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Banking Corporate Lending accessible data. CVSS 3.0 Base Score 5.3	NA	**A-Ora-Banki/01-08-18/101**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			(Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE-ID:CVE-2018-3038**		
NA	18-07-2018	**5.5**	Vulnerability in the Oracle Banking Corporate Lending component of Oracle Financial Services Applications (subcomponent: Core module). Supported versions that are affected are 12.3.0, 12.4.0, 12.5.0, 14.0.0 and 14.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Banking Corporate Lending. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Banking Corporate Lending accessible data as well as unauthorized access to critical data or complete access to all Oracle Banking Corporate Lending accessible data. CVSS 3.0 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N). **CVE-ID:CVE-2018-3050**	NA	**A-Ora-Banki/01-08-18/102**
NA	18-07-2018	**5.5**	Vulnerability in the Oracle Banking Corporate Lending component of Oracle Financial Services Applications (subcomponent: Core module). Supported versions that are affected are 12.3.0, 12.4.0, 12.5.0, 14.0.0 and 14.1.0. Easily exploitable vulnerability	NA	**A-Ora-Banki/01-08-18/103**

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			allows low privileged attacker with network access via HTTP to compromise Oracle Banking Corporate Lending. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Banking Corporate Lending accessible data as well as unauthorized read access to a subset of Oracle Banking Corporate Lending accessible data. CVSS 3.0 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N). **CVE-ID:CVE-2018-3044**		
NA	18-07-2018	**5.8**	Vulnerability in the Oracle Banking Corporate Lending component of Oracle Financial Services Applications (subcomponent: Core module). Supported versions that are affected are 12.3.0, 12.4.0, 12.5.0, 14.0.0 and 14.1.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Banking Corporate Lending. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Banking Corporate Lending, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Banking Corporate Lending	NA	**A-Ora-Banki/01-08-18/104**

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			accessible data as well as unauthorized read access to a subset of Oracle Banking Corporate Lending accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE-ID:CVE-2018-2895**		
Banking Payments					
DoS	18-07-2018	**5.5**	Vulnerability in the Oracle Banking Payments component of Oracle Financial Services Applications (subcomponent: Payments Core). Supported versions that are affected are 12.2.0, 12.3.0, 12.4.0, 12.5.0 and 14.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Banking Payments. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Banking Payments accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Banking Payments. CVSS 3.0 Base Score 5.4 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:L). **CVE-ID:CVE-2018-3023**	NA	**A-Ora-Banki/01-08-18/105**
DoS	18-07-2018	**6.5**	Vulnerability in the Oracle Banking Payments component of Oracle Financial Services Applications (subcomponent: Payments Core). Supported	NA	**A-Ora-Banki/01-08-18/106**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			versions that are affected are 12.2.0, 12.3.0, 12.4.0, 12.5.0 and 14.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Banking Payments. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Banking Payments accessible data as well as unauthorized read access to a subset of Oracle Banking Payments accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Banking Payments. CVSS 3.0 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L). **CVE-ID:CVE-2018-3020**		
NA	18-07-2018	**3.5**	Vulnerability in the Oracle Banking Payments component of Oracle Financial Services Applications (subcomponent: Payments Core). Supported versions that are affected are 12.2.0, 12.3.0, 12.4.0, 12.5.0 and 14.1.0. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Banking Payments. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Banking Payments accessible data. CVSS 3.0 Base	NA	**A-Ora-Banki/01-08-18/107**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N). **CVE-ID:CVE-2018-3025**		
NA	18-07-2018	**4**	Vulnerability in the Oracle Banking Payments component of Oracle Financial Services Applications (subcomponent: Payments Core). Supported versions that are affected are 12.2.0, 12.3.0, 12.4.0, 12.5.0 and 14.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Banking Payments. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Banking Payments. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). **CVE-ID:CVE-2018-3022**	NA	**A-Ora-Banki/01-08-18/108**
NA	18-07-2018	**4.9**	Vulnerability in the Oracle Banking Payments component of Oracle Financial Services Applications (subcomponent: Payments Core). Supported versions that are affected are 12.2.0, 12.3.0, 12.4.0, 12.5.0 and 14.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Banking Payments. Successful attacks require human interaction from a person other than the	NA	**A-Ora-Banki/01-08-18/109**

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			attacker and while the vulnerability is in Oracle Banking Payments, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Banking Payments accessible data as well as unauthorized read access to a subset of Oracle Banking Payments accessible data. CVSS 3.0 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N). **CVE-ID:CVE-2018-3026**		
NA	18-07-2018	**5**	Vulnerability in the Oracle Banking Payments component of Oracle Financial Services Applications (subcomponent: Payments Core). Supported versions that are affected are 12.2.0, 12.3.0, 12.4.0, 12.5.0 and 14.1.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Banking Payments. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Banking Payments accessible data. CVSS 3.0 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE-ID:CVE-2018-3021**	NA	**A-Ora-Banki/01-08-18/110**

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
NA	18-07-2018	**5.5**	Vulnerability in the Oracle Banking Payments component of Oracle Financial Services Applications (subcomponent: Payments Core). Supported versions that are affected are 12.2.0, 12.3.0, 12.4.0, 12.5.0 and 14.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Banking Payments. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Banking Payments accessible data as well as unauthorized access to critical data or complete access to all Oracle Banking Payments accessible data. CVSS 3.0 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N). **CVE-ID:CVE-2018-3027**	NA	**A-Ora-Banki/01-08-18/111**
NA	18-07-2018	**5.5**	Vulnerability in the Oracle Banking Payments component of Oracle Financial Services Applications (subcomponent: Payments Core). Supported versions that are affected are 12.2.0, 12.3.0, 12.4.0, 12.5.0 and 14.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Banking Payments. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of	NA	**A-Ora-Banki/01-08-18/112**

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			Oracle Banking Payments accessible data as well as unauthorized read access to a subset of Oracle Banking Payments accessible data. CVSS 3.0 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N). **CVE-ID:CVE-2018-3024**		
NA	18-07-2018	**5.8**	Vulnerability in the Oracle Banking Payments component of Oracle Financial Services Applications (subcomponent: Payments Core). Supported versions that are affected are 12.2.0, 12.3.0, 12.4.0, 12.5.0 and 14.1.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Banking Payments. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Banking Payments, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Banking Payments accessible data as well as unauthorized read access to a subset of Oracle Banking Payments accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	NA	**A-Ora-Banki/01-08-18/113**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			CVE-ID:CVE-2018-2896		
Business Intelligence Publisher					
NA	18-07-2018	**4**	Vulnerability in the BI Publisher component of Oracle Fusion Middleware (subcomponent: Web Server). Supported versions that are affected are 11.1.1.7.0, 11.1.1.9.0, 12.2.1.2.0 and 12.2.1.3.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise BI Publisher. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all BI Publisher accessible data. CVSS 3.0 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N). **CVE-ID:CVE-2018-2925**	NA	**A-Ora-Busin/01-08-18/114**
NA	18-07-2018	**6.4**	Vulnerability in the BI Publisher component of Oracle Fusion Middleware (subcomponent: BI Publisher Security). Supported versions that are affected are 11.1.1.7.0, 11.1.1.9.0, 12.2.1.2.0 and 12.2.1.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise BI Publisher. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all BI Publisher accessible data as well as unauthorized read	NA	**A-Ora-Busin/01-08-18/115**

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			access to a subset of BI Publisher accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:N). **CVE-ID:CVE-2018-2958**		
NA	18-07-2018	**6.4**	Vulnerability in the BI Publisher component of Oracle Fusion Middleware (subcomponent: Layout Tools). The supported version that is affected is 11.1.1.7.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise BI Publisher. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all BI Publisher accessible data as well as unauthorized read access to a subset of BI Publisher accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:N). **CVE-ID:CVE-2018-2900**	NA	**A-Ora-Busin/01-08-18/116**
Business Process Management Suite					
NA	18-07-2018	**6.4**	Vulnerability in the Oracle Business Process Management Suite component of Oracle Fusion Middleware (subcomponent: Process Analysis & Discovery). Supported versions that are affected are 11.1.1.7.0, 11.1.1.9.0, 12.1.3.0.0, 12.2.1.2.0 and 12.2.1.3.0. Easily	NA	**A-Ora-Busin/01-08-18/117**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Business Process Management Suite. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Business Process Management Suite accessible data as well as unauthorized access to critical data or complete access to all Oracle Business Process Management Suite accessible data. CVSS 3.0 Base Score 9.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N). **CVE-ID:CVE-2018-3100**		
Communications Convergence					
NA	18-07-2018	**5.8**	Vulnerability in the Oracle Communications Messaging Server component of Oracle Communications Applications (subcomponent: Web Client). The supported version that is affected is 3.x. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Communications Messaging Server. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Communications Messaging Server, attacks may significantly impact additional	NA	**A-Ora-Commu/01-08-18/118**

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Communications Messaging Server accessible data as well as unauthorized read access to a subset of Oracle Communications Messaging Server accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE-ID:CVE-2018-2936**		
Communications Eagle Local Number Portability Application Processor					
NA	18-07-2018	**6.4**	Vulnerability in the Oracle Communications EAGLE LNP Application Processor component of Oracle Communications Applications (subcomponent: GUI). The supported version that is affected is 10.x. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Communications EAGLE LNP Application Processor. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Communications EAGLE LNP Application Processor accessible data as well as unauthorized read access to a subset of Oracle Communications EAGLE LNP Application Processor accessible data. CVSS 3.0 Base Score 6.5 (Confidentiality and	NA	**A-Ora-Commu/01-08-18/119**

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N). **CVE-ID:CVE-2018-2904**		
Customer Relationship Management Technical Foundation					
NA	18-07-2018	**5.8**	Vulnerability in the Oracle CRM Technical Foundation component of Oracle E-Business Suite (subcomponent: Preferences). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6 and 12.2.7. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle CRM Technical Foundation. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle CRM Technical Foundation, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle CRM Technical Foundation accessible data as well as unauthorized update, insert or delete access to some of Oracle CRM Technical Foundation accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N). **CVE-ID:CVE-2018-2993**	NA	**A-Ora-Custo/01-08-18/120**

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
NA	18-07-2018	**5.8**	Vulnerability in the Oracle CRM Technical Foundation component of Oracle E-Business Suite (subcomponent: Preferences). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6 and 12.2.7. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle CRM Technical Foundation. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle CRM Technical Foundation, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle CRM Technical Foundation accessible data as well as unauthorized update, insert or delete access to some of Oracle CRM Technical Foundation accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N). **CVE-ID:CVE-2018-3017**	NA	**A-Ora-Custo/01-08-18/121**
Database Server					
NA	18-07-2018	**3.5**	Vulnerability in the Java VM component of Oracle Database Server. Supported versions that are affected are 11.2.0.4, 12.1.0.2,12.2.0.1 and 18.2.	NA	**A-Ora-Datab/01-08-18/122**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			Difficult to exploit vulnerability allows low privileged attacker having Create Session, Create Procedure privilege with network access via multiple protocols to compromise Java VM. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Java VM accessible data. CVSS 3.0 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N). **CVE-ID:CVE-2018-3004**		
NA	18-07-2018	**3.6**	Vulnerability in the Core RDBMS component of Oracle Database Server. Supported versions that are affected are 11.2.0.4, 12.1.0.2, 12.2.0.1, 18.1 and 18.2. Easily exploitable vulnerability allows low privileged attacker having Local Logon privilege with logon to the infrastructure where Core RDBMS executes to compromise Core RDBMS. While the vulnerability is in Core RDBMS, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Core RDBMS accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Core RDBMS. CVSS 3.0 Base Score 8.4 (Integrity and Availability	NA	**A-Ora-Datab/01-08-18/123**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:N/I:H/A:H). **CVE-ID:CVE-2018-2939**		
E-business Suite					
NA	18-07-2018	**5**	Vulnerability in the Oracle Application Object Library component of Oracle E-Business Suite (subcomponent: Attachments / File Upload). The supported version that is affected is 12.1.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Application Object Library. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Application Object Library accessible data. CVSS 3.0 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE-ID:CVE-2018-2934**	NA	**A-Ora-E-bus/01-08-18/124**
Enterprise Manager Ops Center					
NA	18-07-2018	**6.4**	Vulnerability in the Enterprise Manager Ops Center component of Oracle Enterprise Manager Products Suite (subcomponent: Networking). The supported version that is affected is 12.2.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Enterprise Manager Ops Center. Successful attacks of this	NA	**A-Ora-Enter/01-08-18/125**

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			vulnerability can result in unauthorized access to critical data or complete access to all Enterprise Manager Ops Center accessible data as well as unauthorized update, insert or delete access to some of Enterprise Manager Ops Center accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N). **CVE-ID:CVE-2018-2976**		
Flexcube Enterprise Limits And Collateral Management					
DoS	18-07-2018	**5.5**	Vulnerability in the Oracle FLEXCUBE Enterprise Limits and Collateral Management component of Oracle Financial Services Applications (subcomponent: Infrastructure). Supported versions that are affected are 12.3.0, 14.0.0 and 14.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle FLEXCUBE Enterprise Limits and Collateral Management. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle FLEXCUBE Enterprise Limits and Collateral Management accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle FLEXCUBE Enterprise Limits and Collateral Management. CVSS 3.0 Base Score 5.4	NA	**A-Ora-Flexc/01-08-18/126**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			(Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:L). **CVE-ID:CVE-2018-3043**		
DoS	18-07-2018	**6.5**	Vulnerability in the Oracle FLEXCUBE Enterprise Limits and Collateral Management component of Oracle Financial Services Applications (subcomponent: Infrastructure). Supported versions that are affected are 12.3.0, 14.0.0 and 14.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle FLEXCUBE Enterprise Limits and Collateral Management. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle FLEXCUBE Enterprise Limits and Collateral Management accessible data as well as unauthorized read access to a subset of Oracle FLEXCUBE Enterprise Limits and Collateral Management accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle FLEXCUBE Enterprise Limits and Collateral Management. CVSS 3.0 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L). **CVE-ID:CVE-2018-3037**	NA	**A-Ora-Flexc/01-08-18/127**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
NA	18-07-2018	**3.5**	Vulnerability in the Oracle FLEXCUBE Enterprise Limits and Collateral Management component of Oracle Financial Services Applications (subcomponent: Infrastructure). Supported versions that are affected are 12.3.0, 14.0.0 and 14.1.0. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle FLEXCUBE Enterprise Limits and Collateral Management. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle FLEXCUBE Enterprise Limits and Collateral Management accessible data. CVSS 3.0 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N). **CVE-ID:CVE-2018-3047**	NA	**A-Ora-Flexc/01-08-18/128**
NA	18-07-2018	**4**	Vulnerability in the Oracle FLEXCUBE Enterprise Limits and Collateral Management component of Oracle Financial Services Applications (subcomponent: Infrastructure). Supported versions that are affected are 12.3.0, 14.0.0 and 14.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle FLEXCUBE Enterprise Limits and Collateral Management.	NA	**A-Ora-Flexc/01-08-18/129**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle FLEXCUBE Enterprise Limits and Collateral Management. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). **CVE-ID:CVE-2018-3041**		
NA	18-07-2018	**4.9**	Vulnerability in the Oracle FLEXCUBE Enterprise Limits and Collateral Management component of Oracle Financial Services Applications (subcomponent: Infrastructure). Supported versions that are affected are 12.3.0, 14.0.0 and 14.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle FLEXCUBE Enterprise Limits and Collateral Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle FLEXCUBE Enterprise Limits and Collateral Management, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle FLEXCUBE Enterprise Limits and Collateral Management accessible data as well as	NA	**A-Ora-Flexc/01-08-18/130**

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			unauthorized read access to a subset of Oracle FLEXCUBE Enterprise Limits and Collateral Management accessible data. CVSS 3.0 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N). **CVE-ID:CVE-2018-3049**		
NA	18-07-2018	**5**	Vulnerability in the Oracle FLEXCUBE Enterprise Limits and Collateral Management component of Oracle Financial Services Applications (subcomponent: Infrastructure). Supported versions that are affected are 12.3.0, 14.0.0 and 14.1.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle FLEXCUBE Enterprise Limits and Collateral Management. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle FLEXCUBE Enterprise Limits and Collateral Management accessible data. CVSS 3.0 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE-ID:CVE-2018-3039**	NA	**A-Ora-Flexc/01-08-18/131**
NA	18-07-2018	**5.5**	Vulnerability in the Oracle FLEXCUBE Enterprise Limits and Collateral Management component of Oracle Financial Services Applications (subcomponent:	NA	**A-Ora-Flexc/01-08-18/132**

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			Infrastructure). Supported versions that are affected are 12.3.0, 14.0.0 and 14.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle FLEXCUBE Enterprise Limits and Collateral Management. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle FLEXCUBE Enterprise Limits and Collateral Management accessible data as well as unauthorized access to critical data or complete access to all Oracle FLEXCUBE Enterprise Limits and Collateral Management accessible data. CVSS 3.0 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N). **CVE-ID:CVE-2018-3051**		
NA	18-07-2018	**5.5**	Vulnerability in the Oracle FLEXCUBE Enterprise Limits and Collateral Management component of Oracle Financial Services Applications (subcomponent: Infrastructure). Supported versions that are affected are 12.3.0, 14.0.0 and 14.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle FLEXCUBE Enterprise Limits and Collateral Management. Successful attacks of this	NA	**A-Ora-Flexc/01-08-18/133**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			vulnerability can result in unauthorized update, insert or delete access to some of Oracle FLEXCUBE Enterprise Limits and Collateral Management accessible data as well as unauthorized read access to a subset of Oracle FLEXCUBE Enterprise Limits and Collateral Management accessible data. CVSS 3.0 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N). **CVE-ID:CVE-2018-3045**		
NA	18-07-2018	**5.8**	Vulnerability in the Oracle FLEXCUBE Enterprise Limits and Collateral Management component of Oracle Financial Services Applications (subcomponent: Infrastructure). Supported versions that are affected are 12.3.0, 14.0.0 and 14.1.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle FLEXCUBE Enterprise Limits and Collateral Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle FLEXCUBE Enterprise Limits and Collateral Management, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or	NA	**A-Ora-Flexc/01-08-18/134**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			delete access to some of Oracle FLEXCUBE Enterprise Limits and Collateral Management accessible data as well as unauthorized read access to a subset of Oracle FLEXCUBE Enterprise Limits and Collateral Management accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE-ID:CVE-2018-2897**		
Flexcube Investor Servicing					
DoS	18-07-2018	**5.5**	Vulnerability in the Oracle FLEXCUBE Investor Servicing component of Oracle Financial Services Applications (subcomponent: Infrastructure). Supported versions that are affected are 12.0.4, 12.1.0, 12.3.0 and 12.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle FLEXCUBE Investor Servicing. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle FLEXCUBE Investor Servicing accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle FLEXCUBE Investor Servicing. CVSS 3.0 Base Score 5.4 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:L).	NA	**A-Ora-Flexc/01-08-18/135**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			CVE-ID:CVE-2018-3031		
DoS	18-07-2018	**6.5**	Vulnerability in the Oracle FLEXCUBE Investor Servicing component of Oracle Financial Services Applications (subcomponent: Infrastructure). Supported versions that are affected are 12.0.4, 12.1.0, 12.3.0 and 12.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle FLEXCUBE Investor Servicing. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle FLEXCUBE Investor Servicing accessible data as well as unauthorized read access to a subset of Oracle FLEXCUBE Investor Servicing accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle FLEXCUBE Investor Servicing. CVSS 3.0 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L). **CVE-ID:CVE-2018-3028**	NA	**A-Ora-Flexc/01-08-18/136**
NA	18-07-2018	**3.5**	Vulnerability in the Oracle FLEXCUBE Investor Servicing component of Oracle Financial Services Applications (subcomponent: Infrastructure). Supported versions that are affected are 12.0.4, 12.1.0, 12.3.0 and 12.4.0. Difficult to exploit	NA	**A-Ora-Flexc/01-08-18/137**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle FLEXCUBE Investor Servicing. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle FLEXCUBE Investor Servicing accessible data. CVSS 3.0 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N). **CVE-ID:CVE-2018-3033**		
NA	18-07-2018	**4**	Vulnerability in the Oracle FLEXCUBE Investor Servicing component of Oracle Financial Services Applications (subcomponent: Infrastructure). Supported versions that are affected are 12.0.4, 12.1.0, 12.3.0 and 12.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle FLEXCUBE Investor Servicing. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle FLEXCUBE Investor Servicing. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). **CVE-ID:CVE-2018-3030**	NA	**A-Ora-Flexc/01-08-18/138**
NA	18-07-2018	**4.9**	Vulnerability in the Oracle FLEXCUBE Investor Servicing component of Oracle Financial	NA	**A-Ora-Flexc/01-08-**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			Services Applications (subcomponent: Infrastructure). Supported versions that are affected are 12.0.4, 12.1.0, 12.3.0 and 12.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle FLEXCUBE Investor Servicing. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle FLEXCUBE Investor Servicing, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle FLEXCUBE Investor Servicing accessible data as well as unauthorized read access to a subset of Oracle FLEXCUBE Investor Servicing accessible data. CVSS 3.0 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N). **CVE-ID:CVE-2018-3034**		**18/139**
NA	18-07-2018	**5**	Vulnerability in the Oracle FLEXCUBE Investor Servicing component of Oracle Financial Services Applications (subcomponent: Infrastructure). Supported versions that are affected are 12.0.4, 12.1.0, 12.3.0 and 12.4.0. Easily exploitable vulnerability allows unauthenticated attacker with	NA	**A-Ora-Flexc/01-08-18/140**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			network access via HTTP to compromise Oracle FLEXCUBE Investor Servicing. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle FLEXCUBE Investor Servicing accessible data. CVSS 3.0 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE-ID:CVE-2018-3029**		
NA	18-07-2018	**5.5**	Vulnerability in the Oracle FLEXCUBE Investor Servicing component of Oracle Financial Services Applications (subcomponent: Infrastructure). Supported versions that are affected are 12.0.4, 12.1.0, 12.3.0 and 12.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle FLEXCUBE Investor Servicing. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle FLEXCUBE Investor Servicing accessible data as well as unauthorized access to critical data or complete access to all Oracle FLEXCUBE Investor Servicing accessible data. CVSS 3.0 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N). **CVE-ID:CVE-2018-3035**	NA	**A-Ora-Flexc/01-08-18/141**

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
NA	18-07-2018	**5.5**	Vulnerability in the Oracle FLEXCUBE Investor Servicing component of Oracle Financial Services Applications (subcomponent: Infrastructure). Supported versions that are affected are 12.0.4, 12.1.0, 12.3.0 and 12.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle FLEXCUBE Investor Servicing. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle FLEXCUBE Investor Servicing accessible data as well as unauthorized read access to a subset of Oracle FLEXCUBE Investor Servicing accessible data. CVSS 3.0 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N). **CVE-ID:CVE-2018-3032**	NA	**A-Ora-Flexc/01-08-18/142**
NA	18-07-2018	**5.8**	Vulnerability in the Oracle FLEXCUBE Investor Servicing component of Oracle Financial Services Applications (subcomponent: Infrastructure). Supported versions that are affected are 12.0.4, 12.1.0, 12.3.0 and 12.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle FLEXCUBE Investor Servicing. Successful attacks require human	NA	**A-Ora-Flexc/01-08-18/143**

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			interaction from a person other than the attacker and while the vulnerability is in Oracle FLEXCUBE Investor Servicing, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle FLEXCUBE Investor Servicing accessible data as well as unauthorized read access to a subset of Oracle FLEXCUBE Investor Servicing accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE-ID:CVE-2018-2898**		
Flexcube Universal Banking					
DoS	18-07-2018	**5.5**	Vulnerability in the Oracle FLEXCUBE Universal Banking component of Oracle Financial Services Applications (subcomponent: Infrastructure). Supported versions that are affected are 11.3.0, 11.4.0, 12.0.1, 12.0.2, 12.0.3, 12.1.0, 12.2.0, 12.3.0, 12.4.0, 14.0.0 and 14.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle FLEXCUBE Universal Banking. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle FLEXCUBE Universal Banking accessible data and unauthorized ability to cause a	NA	**A-Ora-Flexc/01-08-18/144**

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			partial denial of service (partial DOS) of Oracle FLEXCUBE Universal Banking. CVSS 3.0 Base Score 5.4 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:L). **CVE-ID:CVE-2018-2980**		
DoS	18-07-2018	**6.5**	Vulnerability in the Oracle FLEXCUBE Universal Banking component of Oracle Financial Services Applications (subcomponent: Infrastructure). Supported versions that are affected are 11.3.0, 11.4.0, 12.0.1, 12.0.2, 12.0.3, 12.1.0, 12.2.0, 12.3.0, 12.4.0, 14.0.0 and 14.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle FLEXCUBE Universal Banking. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle FLEXCUBE Universal Banking accessible data as well as unauthorized read access to a subset of Oracle FLEXCUBE Universal Banking accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle FLEXCUBE Universal Banking. CVSS 3.0 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L). **CVE-ID:CVE-2018-2974**	NA	**A-Ora-Flexc/01-08-18/145**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
NA	18-07-2018	**3.5**	Vulnerability in the Oracle FLEXCUBE Universal Banking component of Oracle Financial Services Applications (subcomponent: Infrastructure). Supported versions that are affected are 11.3.0, 11.4.0, 12.0.1, 12.0.2, 12.0.3, 12.1.0, 12.2.0, 12.3.0, 12.4.0, 14.0.0 and 14.1.0. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle FLEXCUBE Universal Banking. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle FLEXCUBE Universal Banking accessible data. CVSS 3.0 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N). **CVE-ID:CVE-2018-2982**	NA	**A-Ora-Flexc/01-08-18/146**
NA	18-07-2018	**4**	Vulnerability in the Oracle FLEXCUBE Universal Banking component of Oracle Financial Services Applications (subcomponent: Infrastructure). Supported versions that are affected are 11.3.0, 11.4.0, 12.0.1, 12.0.2, 12.0.3, 12.1.0, 12.2.0, 12.3.0, 12.4.0, 14.0.0 and 14.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle FLEXCUBE Universal Banking. Successful attacks of this vulnerability can result in	NA	**A-Ora-Flexc/01-08-18/147**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle FLEXCUBE Universal Banking. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). **CVE-ID:CVE-2018-2979**		
NA	18-07-2018	**4.9**	Vulnerability in the Oracle FLEXCUBE Universal Banking component of Oracle Financial Services Applications (subcomponent: Infrastructure). Supported versions that are affected are 11.3.0, 11.4.0, 12.0.1, 12.0.2, 12.0.3, 12.1.0, 12.2.0, 12.3.0, 12.4.0, 14.0.0 and 14.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle FLEXCUBE Universal Banking. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle FLEXCUBE Universal Banking, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle FLEXCUBE Universal Banking accessible data as well as unauthorized read access to a subset of Oracle FLEXCUBE Universal Banking accessible data. CVSS 3.0 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector:	NA	**A-Ora-Flexc/01-08-18/148**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			(CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N). **CVE-ID:CVE-2018-3019**		
NA	18-07-2018	**5**	Vulnerability in the Oracle FLEXCUBE Universal Banking component of Oracle Financial Services Applications (subcomponent: Infrastructure). Supported versions that are affected are 11.3.0, 11.4.0, 12.0.1, 12.0.2, 12.0.3, 12.1.0, 12.2.0, 12.3.0, 12.4.0, 14.0.0 and 14.1.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle FLEXCUBE Universal Banking. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle FLEXCUBE Universal Banking accessible data. CVSS 3.0 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE-ID:CVE-2018-2975**	NA	**A-Ora-Flexc/01-08-18/149**
NA	18-07-2018	**5.5**	Vulnerability in the Oracle FLEXCUBE Universal Banking component of Oracle Financial Services Applications (subcomponent: Infrastructure). Supported versions that are affected are 11.3.0, 11.4.0, 12.0.1, 12.0.2, 12.0.3, 12.1.0, 12.2.0, 12.3.0, 12.4.0, 14.0.0 and 14.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle FLEXCUBE Universal Banking.	NA	**A-Ora-Flexc/01-08-18/150**

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle FLEXCUBE Universal Banking accessible data as well as unauthorized access to critical data or complete access to all Oracle FLEXCUBE Universal Banking accessible data. CVSS 3.0 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N). **CVE-ID:CVE-2018-3015**		
NA	18-07-2018	**5.5**	Vulnerability in the Oracle FLEXCUBE Universal Banking component of Oracle Financial Services Applications (subcomponent: Infrastructure). Supported versions that are affected are 11.3.0, 11.4.0, 12.0.1, 12.0.2, 12.0.3, 12.1.0, 12.2.0, 12.3.0, 12.4.0, 14.0.0 and 14.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle FLEXCUBE Universal Banking. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle FLEXCUBE Universal Banking accessible data as well as unauthorized read access to a subset of Oracle FLEXCUBE Universal Banking accessible data. CVSS 3.0 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector:	NA	**A-Ora-Flexc/01-08-18/151**

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			(CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N). **CVE-ID:CVE-2018-2981**		
NA	18-07-2018	**5.8**	Vulnerability in the Oracle FLEXCUBE Universal Banking component of Oracle Financial Services Applications (subcomponent: Infrastructure). Supported versions that are affected are 11.3.0, 11.4.0, 12.0.1, 12.0.2, 12.0.3, 12.1.0, 12.2.0, 12.3.0, 12.4.0, 14.0.0 and 14.1.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle FLEXCUBE Universal Banking. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle FLEXCUBE Universal Banking, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle FLEXCUBE Universal Banking accessible data as well as unauthorized read access to a subset of Oracle FLEXCUBE Universal Banking accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE-ID:CVE-2018-2899**	NA	**A-Ora-Flexc/01-08-18/152**
Fusion Middleware Mapviewer					
NA	18-07-2018	**7.5**	Vulnerability in the Oracle Fusion Middleware	NA	**A-Ora-Fusio/01-**

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			MapViewer component of Oracle Fusion Middleware (subcomponent: Map Builder). Supported versions that are affected are 12.2.1.2.0 and 12.2.1.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Fusion Middleware MapViewer. Successful attacks of this vulnerability can result in takeover of Oracle Fusion Middleware MapViewer. CVSS 3.0 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H). **CVE-ID:CVE-2018-2943**		**08-18/153**
Hardware Management Pack					
NA	18-07-2018	**4.3**	Vulnerability in the Hardware Management Pack component of Oracle Sun Systems Products Suite (subcomponent: Ipmitool). The supported version that is affected is 11.3. Difficult to exploit vulnerability allows unauthenticated attacker with network access via IPMI to compromise Hardware Management Pack. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Hardware Management Pack accessible data. CVSS 3.0 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N).	NA	**A-Ora-Hardw/01-08-18/154**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			CVE-ID:CVE-2018-2906		
Hospitality Cruise Fleet Management					
NA	18-07-2018	**5.5**	Vulnerability in the Oracle Hospitality Cruise Fleet Management System component of Oracle Hospitality Applications (subcomponent: Gangway Activity Web App). The supported version that is affected is 9.x. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hospitality Cruise Fleet Management System. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hospitality Cruise Fleet Management System accessible data as well as unauthorized access to critical data or complete access to all Oracle Hospitality Cruise Fleet Management System accessible data. CVSS 3.0 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N). **CVE-ID:CVE-2018-2984**	NA	**A-Ora-Hospi/01-08-18/155**
Hospitality Opera Property Management					
NA	18-07-2018	**4**	Vulnerability in the Oracle Hospitality OPERA 5 Property Services component of Oracle Hospitality Applications (subcomponent: Report Server Config). The supported version that is affected is 5.5.x. Easily	NA	**A-Ora-Hospi/01-08-18/156**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hospitality OPERA 5 Property Services. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hospitality OPERA 5 Property Services accessible data. CVSS 3.0 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N). **CVE-ID:CVE-2018-3013**		
NA	18-07-2018	**4**	Vulnerability in the Oracle Hospitality OPERA 5 Property Services component of Oracle Hospitality Applications (subcomponent: Reports). The supported version that is affected is 5.5.x. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hospitality OPERA 5 Property Services. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hospitality OPERA 5 Property Services accessible data. CVSS 3.0 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N). **CVE-ID:CVE-2018-3014**	NA	**A-Ora-Hospi/01-08-18/157**

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
NA	18-07-2018	**4.4**	Vulnerability in the Oracle Hospitality OPERA 5 Property Services component of Oracle Hospitality Applications (subcomponent: Integration). The supported version that is affected is 5.5.x. Difficult to exploit vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle Hospitality OPERA 5 Property Services executes to compromise Oracle Hospitality OPERA 5 Property Services. While the vulnerability is in Oracle Hospitality OPERA 5 Property Services, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle Hospitality OPERA 5 Property Services. CVSS 3.0 Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H). **CVE-ID:CVE-2018-2956**	NA	**A-Ora-Hospi/01-08-18/158**
NA	18-07-2018	**5**	Vulnerability in the Oracle Hospitality OPERA 5 Property Services component of Oracle Hospitality Applications (subcomponent: Integration). The supported version that is affected is 5.5.x. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hospitality OPERA 5 Property Services. Successful attacks of this vulnerability can	NA	**A-Ora-Hospi/01-08-18/159**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			result in unauthorized read access to a subset of Oracle Hospitality OPERA 5 Property Services accessible data. CVSS 3.0 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE-ID:CVE-2018-2955**		
NA	18-07-2018	**5**	Vulnerability in the Oracle Hospitality OPERA 5 Property Services component of Oracle Hospitality Applications (subcomponent: Logging). The supported version that is affected is 5.5.x. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hospitality OPERA 5 Property Services. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hospitality OPERA 5 Property Services accessible data. CVSS 3.0 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE-ID:CVE-2018-2957**	NA	**A-Ora-Hospi/01-08-18/160**
Hospitality Simphony					
DoS	18-07-2018	**6**	Vulnerability in the Oracle Hospitality Simphony component of Oracle Hospitality Applications (subcomponent: Import/Export). Supported versions that are affected are 2.8, 2.9 and 2.10. Difficult to exploit vulnerability allows	NA	**A-Ora-Hospi/01-08-18/161**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			low privileged attacker with network access via HTTP to compromise Oracle Hospitality Simphony. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hospitality Simphony accessible data as well as unauthorized access to critical data or complete access to all Oracle Hospitality Simphony accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Hospitality Simphony. CVSS 3.0 Base Score 7.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:L). **CVE-ID:CVE-2018-2978**		
Hyperion Data Relationship Management					
NA	18-07-2018	**5**	Vulnerability in the Hyperion Data Relationship Management component of Oracle Hyperion (subcomponent: Access and security). The supported version that is affected is 11.1.2.4.330. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Hyperion Data Relationship Management. While the vulnerability is in Hyperion Data Relationship Management, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in	NA	**A-Ora-Hyper/01-08-18/162**

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			unauthorized read access to a subset of Hyperion Data Relationship Management accessible data. CVSS 3.0 Base Score 5.8 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:N/A:N). **CVE-ID:CVE-2018-2915**		
Hyperion Financial Reporting					
NA	18-07-2018	**5**	Vulnerability in the Hyperion Financial Reporting component of Oracle Hyperion (subcomponent: Security Models). The supported version that is affected is 11.1.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Hyperion Financial Reporting. While the vulnerability is in Hyperion Financial Reporting, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Hyperion Financial Reporting accessible data. CVSS 3.0 Base Score 8.6 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N). **CVE-ID:CVE-2018-2907**	NA	**A-Ora-Hyper/01-08-18/163**
Ilearning					
NA	18-07-2018	**5.8**	Vulnerability in the Oracle iLearning component of Oracle iLearning (subcomponent: Learner Administration). The supported version that is affected is 6.2. Easily	NA	**A-Ora-Ilear/01-08-18/164**

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle iLearning. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle iLearning, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle iLearning accessible data as well as unauthorized update, insert or delete access to some of Oracle iLearning accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N). **CVE-ID:CVE-2018-2989**		
Istore					
NA	18-07-2018	**5**	Vulnerability in the Oracle iStore component of Oracle E-Business Suite (subcomponent: Shopping Cart). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6 and 12.2.7. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle iStore. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle iStore accessible data. CVSS 3.0	NA	**A-Ora-Istor/01-08-18/165**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE-ID:CVE-2018-2994**		
NA	18-07-2018	**5.8**	Vulnerability in the Oracle iStore component of Oracle E-Business Suite (subcomponent: Shopping Cart). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6 and 12.2.7. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle iStore. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle iStore, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle iStore accessible data as well as unauthorized update, insert or delete access to some of Oracle iStore accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N). **CVE-ID:CVE-2018-2995**	NA	**A-Ora-Istor/01-08-18/166**
NA	18-07-2018	**5.8**	Vulnerability in the Oracle iStore component of Oracle E-Business Suite (subcomponent: Shopping Cart). Supported versions that are affected are 12.1.1, 12.1.2,	NA	**A-Ora-Istor/01-08-18/167**

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6 and 12.2.7. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle iStore. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle iStore, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle iStore accessible data as well as unauthorized update, insert or delete access to some of Oracle iStore accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N). **CVE-ID:CVE-2018-3018**		
Jd Edwards Enterpriseone Tools					
NA	18-07-2018	**4**	Vulnerability in the JD Edwards EnterpriseOne Tools component of Oracle JD Edwards Products (subcomponent: Web Runtime). The supported version that is affected is 9.2. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise JD Edwards EnterpriseOne Tools. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all	NA	**A-Ora-Jd/01-08-18/168**

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			JD Edwards EnterpriseOne Tools accessible data. CVSS 3.0 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N). **CVE-ID:CVE-2018-2947**		
NA	18-07-2018	**5**	Vulnerability in the JD Edwards EnterpriseOne Tools component of Oracle JD Edwards Products (subcomponent: Monitoring and Diagnostics). The supported version that is affected is 9.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise JD Edwards EnterpriseOne Tools. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all JD Edwards EnterpriseOne Tools accessible data. CVSS 3.0 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE-ID:CVE-2018-2944**	NA	**A-Ora-Jd/01-08-18/169**
NA	18-07-2018	**5.8**	Vulnerability in the JD Edwards EnterpriseOne Tools component of Oracle JD Edwards Products (subcomponent: Web Runtime). The supported version that is affected is 9.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise JD Edwards EnterpriseOne Tools. Successful attacks require	NA	**A-Ora-Jd/01-08-18/170**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			human interaction from a person other than the attacker and while the vulnerability is in JD Edwards EnterpriseOne Tools, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of JD Edwards EnterpriseOne Tools accessible data as well as unauthorized read access to a subset of JD Edwards EnterpriseOne Tools accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE-ID:CVE-2018-2945**		
NA	18-07-2018	**5.8**	Vulnerability in the JD Edwards EnterpriseOne Tools component of Oracle JD Edwards Products (subcomponent: Web Runtime). The supported version that is affected is 9.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise JD Edwards EnterpriseOne Tools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in JD Edwards EnterpriseOne Tools, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of JD	NA	**A-Ora-Jd/01-08-18/171**

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			Edwards EnterpriseOne Tools accessible data as well as unauthorized read access to a subset of JD Edwards EnterpriseOne Tools accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE-ID:CVE-2018-2946**		
NA	18-07-2018	**5.8**	Vulnerability in the JD Edwards EnterpriseOne Tools component of Oracle JD Edwards Products (subcomponent: Web Runtime). The supported version that is affected is 9.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise JD Edwards EnterpriseOne Tools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in JD Edwards EnterpriseOne Tools, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of JD Edwards EnterpriseOne Tools accessible data as well as unauthorized read access to a subset of JD Edwards EnterpriseOne Tools accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	NA	**A-Ora-Jd/01-08-18/172**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			CVE-ID:CVE-2018-2948		
NA	18-07-2018	**5.8**	Vulnerability in the JD Edwards EnterpriseOne Tools component of Oracle JD Edwards Products (subcomponent: Web Runtime). The supported version that is affected is 9.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise JD Edwards EnterpriseOne Tools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in JD Edwards EnterpriseOne Tools, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of JD Edwards EnterpriseOne Tools accessible data as well as unauthorized read access to a subset of JD Edwards EnterpriseOne Tools accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE-ID:CVE-2018-2949**	NA	**A-Ora-Jd/01-08-18/173**
NA	18-07-2018	**5.8**	Vulnerability in the JD Edwards EnterpriseOne Tools component of Oracle JD Edwards Products (subcomponent: Web Runtime). The supported version that is affected is 9.2. Easily exploitable vulnerability allows unauthenticated	NA	**A-Ora-Jd/01-08-18/174**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			attacker with network access via HTTP to compromise JD Edwards EnterpriseOne Tools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in JD Edwards EnterpriseOne Tools, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of JD Edwards EnterpriseOne Tools accessible data as well as unauthorized read access to a subset of JD Edwards EnterpriseOne Tools accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE-ID:CVE-2018-2950**		
NA	18-07-2018	**5.8**	Vulnerability in the JD Edwards EnterpriseOne Tools component of Oracle JD Edwards Products (subcomponent: Web Runtime). The supported version that is affected is 9.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise JD Edwards EnterpriseOne Tools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in JD Edwards EnterpriseOne Tools, attacks may significantly impact additional products.	NA	**A-Ora-Jd/01-08-18/175**

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of JD Edwards EnterpriseOne Tools accessible data as well as unauthorized read access to a subset of JD Edwards EnterpriseOne Tools accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE-ID:CVE-2018-2999**		
NA	18-07-2018	**5.8**	Vulnerability in the JD Edwards EnterpriseOne Tools component of Oracle JD Edwards Products (subcomponent: Web Runtime). The supported version that is affected is 9.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise JD Edwards EnterpriseOne Tools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in JD Edwards EnterpriseOne Tools, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of JD Edwards EnterpriseOne Tools accessible data as well as unauthorized read access to a subset of JD Edwards EnterpriseOne Tools accessible data. CVSS 3.0 Base Score 6.1	NA	**A-Ora-Jd/01-08-18/176**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			(Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE-ID:CVE-2018-3006**		
JDK,JRE					
NA	18-07-2018	**4.3**	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: Security). The supported version that is affected is Java SE: 10.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Java SE accessible data. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 5.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE-ID:CVE-2018-2972**	https://security.netapp.com/advisory/ntap-20180726-0001/	**A-Ora-JDK,J/01-08-18/178**
NA	18-07-2018	**4.3**	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: JSSE). Supported versions that are	https://security.netapp.com/advisory/ntap-20180726-0001/,	**A-Ora-JDK,J/01-08-18/179**

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			affected are Java SE: 6u191, 7u181, 8u172 and 10.0.1; Java SE Embedded: 8u171. Difficult to exploit vulnerability allows unauthenticated attacker with network access via SSL/TLS to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 5.9 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N). **CVE-ID:CVE-2018-2973**	https://access.redhat.com/errata/RHSA-2018:2253, https://access.redhat.com/errata/RHSA-2018:2254, https://access.redhat.com/errata/RHSA-2018:2255, https://access.redhat.com/errata/RHSA-2018:2256	
NA	18-07-2018	**4.3**	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Libraries). Supported versions that are affected are Java SE: 6u191, 7u181, 8u172 and 10.0.1; Java SE Embedded: 8u171. Easily exploitable vulnerability allows unauthenticated	https://access.redhat.com/errata/RHSA-2018:2255, https://access.redhat.com/errata/RHSA-2018:2256, https://security.netapp.com/adviso	**A-Ora-JDK,J/01-08-18/180**

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N). **CVE-ID:CVE-2018-2940**	ry/ntap-20180726-0001/, https://access.redhat.com/errata/RHSA-2018:2254, https://access.redhat.com/errata/RHSA-2018:2253	
NA	18-07-2018	**5.1**	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: Deployment). Supported versions that are affected are Java SE: 8u172 and 10.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks require human interaction from a	https://access.redhat.com/errata/RHSA-2018:2256, https://access.redhat.com/errata/RHSA-2018:2253, https://security.netapp.com/advisory/ntap-20180726-0001/	**A-Ora-JDK,J/01-08-18/181**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			person other than the attacker and while the vulnerability is in Java SE, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 8.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H). **CVE-ID:CVE-2018-2964**		
NA	18-07-2018	**5.1**	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: JavaFX). Supported versions that are affected are Java SE: 7u181, 8u172 and 10.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, attacks may significantly impact additional	https://access.redhat.com/errata/RHSA-2018:2256, https://access.redhat.com/errata/RHSA-2018:2253, https://security.netapp.com/advisory/ntap-20180726-0001/, https://access.redhat.com/errata/RHSA-2018:2255,	**A-Ora-JDK,J/01-08-18/182**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			products. Successful attacks of this vulnerability can result in takeover of Java SE. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 8.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H). **CVE-ID:CVE-2018-2941**	https://access.redhat.com/errata/RHSA-2018:2254	
NA	18-07-2018	**5.1**	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: Windows DLL). Supported versions that are affected are Java SE: 7u181 and 8u172. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE. Note: Applies to client and server	https://security.netapp.com/advisory/ntap-20180726-0001/	**A-Ora-JDK,J/01-08-18/183**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 8.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H). **CVE-ID:CVE-2018-2942**		
NA	18-07-2018	**6.8**	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: Java DB). Supported versions that are affected are Java SE: 6u191, 7u181 and 8u172. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. While the vulnerability is in Java SE, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE. Note: This vulnerability can only be exploited by supplying data to APIs in the specified Component without using Untrusted Java Web Start applications or Untrusted Java applets, such as through a web service. CVE-2018-2938 addresses CVE-2018-1313. CVSS 3.0 Base Score 9.0	https://security.netapp.com/advisory/ntap-20180726-0001/	**A-Ora-JDK,J/01-08-18/184**

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			(Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H). **CVE-ID:CVE-2018-2938**		
JDK,JRE,Jrockit					
DoS	18-07-2018	**4.3**	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: Concurrency). Supported versions that are affected are Java SE: 6u191, 7u181, 8u172 and 10.0.1; Java SE Embedded: 8u171; JRockit: R28.3.18. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded, JRockit. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).	https://security.netapp.com/advisory/ntap-20180726-0001/, https://access.redhat.com/errata/RHSA-2018:2254, https://access.redhat.com/errata/RHSA-2018:2255, https://access.redhat.com/errata/RHSA-2018:2256, https://access.redhat.com/errata/RHSA-2018:2241, https://access.redhat.com/errata/RHSA-2018:2253, https://access.redhat.com/errata/RHSA-2018:2242	**A-Ora-JDK,J/01-08-18/177**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			CVE-ID:CVE-2018-2952		
Marketing					
NA	18-07-2018	**4**	Vulnerability in the Oracle Marketing component of Oracle E-Business Suite (subcomponent: Products). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6 and 12.2.7. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Marketing. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Marketing, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Marketing accessible data as well as unauthorized update, insert or delete access to some of Oracle Marketing accessible data. CVSS 3.0 Base Score 6.9 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:L/A:N). **CVE-ID:CVE-2018-2988**	NA	**A-Ora-Marke/01-08-18/185**
NA	18-07-2018	**5.8**	Vulnerability in the Oracle Marketing component of Oracle E-Business Suite (subcomponent: User Interface). Supported versions that are affected are 12.1.1, 12.1.2 and 12.1.3. Easily exploitable vulnerability allows unauthenticated	NA	**A-Ora-Marke/01-08-18/186**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			attacker with network access via HTTP to compromise Oracle Marketing. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Marketing, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Marketing accessible data as well as unauthorized update, insert or delete access to some of Oracle Marketing accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N). **CVE-ID:CVE-2018-3008**		
Micros Relate Customer Relationship Management Software					
DoS	18-07-2018	**5.5**	Vulnerability in the MICROS Relate CRM Software component of Oracle Retail Applications (subcomponent: Internal Operations). Supported versions that are affected are 10.8.x and 11.4.x. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise MICROS Relate CRM Software. While the vulnerability is in MICROS Relate CRM Software, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some	NA	**A-Ora-Micro/01-08-18/187**

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			of MICROS Relate CRM Software accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MICROS Relate CRM Software. CVSS 3.0 Base Score 6.4 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:N/I:L/A:L). **CVE-ID:CVE-2018-3052**		
Micros Retail-j					
DoS	18-07-2018	**3.7**	Vulnerability in the MICROS Retail-J component of Oracle Retail Applications (subcomponent: Back Office). Supported versions that are affected are 10.2.x, 11.0.x, 12.0.x, 12.1.x, 12.1.1.x,12.1.2.x and 13.1.x. Difficult to exploit vulnerability allows physical access to compromise MICROS Retail-J. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in MICROS Retail-J, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all MICROS Retail-J accessible data as well as unauthorized access to critical data or complete access to all MICROS Retail-J accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MICROS Retail-J. CVSS 3.0 Base Score	NA	**A-Ora-Micro/01-08-18/188**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			6.7 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:P/AC:H/PR:H/UI:R/S:C/C:H/I:H/A:L). **CVE-ID:CVE-2018-2888**		
DoS	18-07-2018	**6.5**	Vulnerability in the MICROS Retail-J component of Oracle Retail Applications (subcomponent: Database). Supported versions that are affected are 11.0.x, 12.0.x, 12.1.x, 12.1.1.x, 12.1.2.x and 13.1.x. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise MICROS Retail-J. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MICROS Retail-J accessible data as well as unauthorized read access to a subset of MICROS Retail-J accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MICROS Retail-J. CVSS 3.0 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L). **CVE-ID:CVE-2018-2881**	NA	**A-Ora-Micro/01-08-18/189**
NA	18-07-2018	**4**	Vulnerability in the MICROS Retail-J component of Oracle Retail Applications (subcomponent: Interfaces). Supported versions that are affected are 10.2.x, 11.0.x, 12.0.x,12.1.x, 12.1.1.x,12.1.2.x and 13.1.x. Easily exploitable	NA	**A-Ora-Micro/01-08-18/190**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			vulnerability allows low privileged attacker with network access via HTTP to compromise MICROS Retail-J. While the vulnerability is in MICROS Retail-J, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all MICROS Retail-J accessible data. CVSS 3.0 Base Score 7.7 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:N/I:H/A:N). **CVE-ID:CVE-2018-2882**		
Mysql					
NA	18-07-2018	**3.5**	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Memcached). Supported versions that are affected are 5.6.40 and prior, 5.7.22 and prior and 8.0.11 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via memcached to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H). **CVE-ID:CVE-2018-3062**	https://security.netapp.com/advisory/ntap-20180726-0002/	**A-Ora-Mysql/01-08-18/191**
NA	18-07-2018	**3.5**	Vulnerability in the MySQL Server component of Oracle	https://security.netapp.com/adviso	**A-Ora-Mysql/01**

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			MySQL (subcomponent: Server: Security: Encryption). Supported versions that are affected are 5.5.60 and prior, 5.6.40 and prior and 5.7.22 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.0 Base Score 3.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N). **CVE-ID:CVE-2018-2767**	ry/ntap-20180726-0002/	**-08-18/192**
NA	18-07-2018	**3.5**	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Roles). Supported versions that are affected are 8.0.11 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H). **CVE-ID:CVE-2018-3074**	https://security.netapp.com/advisory/ntap-20180726-0002/	**A-Ora-Mysql/01-08-18/193**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
NA	18-07-2018	**4**	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Audit Log). Supported versions that are affected are 5.7.22 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE-ID:CVE-2018-3071**	https://security.netapp.com/advisory/ntap-20180726-0002/	**A-Ora-Mysql/01-08-18/194**
NA	18-07-2018	**4**	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Client mysqldump). Supported versions that are affected are 5.5.60 and prior, 5.6.40 and prior and 5.7.22 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). **CVE-ID:CVE-2018-3070**	https://security.netapp.com/advisory/ntap-20180726-0002/	**A-Ora-Mysql/01-08-18/195**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
NA	18-07-2018	**4**	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 8.0.11 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE-ID:CVE-2018-3079**	https://security.netapp.com/advisory/ntap-20180726-0002/	**A-Ora-Mysql/01-08-18/196**
NA	18-07-2018	**4**	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: MyISAM). Supported versions that are affected are 5.5.60 and prior, 5.6.40 and prior and 5.7.22 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N). **CVE-ID:CVE-2018-3058**	https://security.netapp.com/advisory/ntap-20180726-0002/	**A-Ora-Mysql/01-08-18/197**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
NA	18-07-2018	**4**	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 5.7.22 and prior and 8.0.11 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE-ID:CVE-2018-3054**	https://security.netapp.com/advisory/ntap-20180726-0002/	**A-Ora-Mysql/01-08-18/198**
NA	18-07-2018	**4**	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 5.7.22 and prior and 8.0.11 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE-ID:CVE-2018-3077**	https://security.netapp.com/advisory/ntap-20180726-0002/	**A-Ora-Mysql/01-08-18/199**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
NA	18-07-2018	**4**	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 8.0.11 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE-ID:CVE-2018-3078**	https://security.netapp.com/advisory/ntap-20180726-0002/	**A-Ora-Mysql/01-08-18/200**
NA	18-07-2018	**4**	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 8.0.11 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE-ID:CVE-2018-3080**	https://security.netapp.com/advisory/ntap-20180726-0002/	**A-Ora-Mysql/01-08-18/201**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
NA	18-07-2018	**4**	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 8.0.11 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.0 Base Score 2.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N). **CVE-ID:CVE-2018-3082**	https://security.netapp.com/advisory/ntap-20180726-0002/	**A-Ora-Mysql/01-08-18/202**
NA	18-07-2018	**4**	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DML). Supported versions that are affected are 5.7.22 and prior and 8.0.11 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). **CVE-ID:CVE-2018-3065**	https://security.netapp.com/advisory/ntap-20180726-0002/	**A-Ora-Mysql/01-08-18/203**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
NA	18-07-2018	**4**	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DML). Supported versions that are affected are 5.7.22 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE-ID:CVE-2018-3061**	https://security.netapp.com/advisory/ntap-20180726-0002/	**A-Ora-Mysql/01-08-18/204**
NA	18-07-2018	**4**	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.11 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). **CVE-ID:CVE-2018-3073**	https://security.netapp.com/advisory/ntap-20180726-0002/	**A-Ora-Mysql/01-08-18/205**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
NA	18-07-2018	**4**	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 8.0.11 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE-ID:CVE-2018-3067**	https://security.netapp.com/advisory/ntap-20180726-0002/	**A-Ora-Mysql/01-08-18/206**
NA	18-07-2018	**4**	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 5.5.60 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE-ID:CVE-2018-3063**	https://security.netapp.com/advisory/ntap-20180726-0002/	**A-Ora-Mysql/01-08-18/207**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
NA	18-07-2018	**4**	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 5.7.22 and prior and 8.0.11 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.0 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N). **CVE-ID:CVE-2018-3056**	https://security.netapp.com/advisory/ntap-20180726-0002/	**A-Ora-Mysql/01-08-18/208**
NA	18-07-2018	**4**	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 8.0.11 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE-ID:CVE-2018-3075**	https://security.netapp.com/advisory/ntap-20180726-0002/	**A-Ora-Mysql/01-08-18/209**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
NA	18-07-2018	**4.9**	Vulnerability in the MySQL Client component of Oracle MySQL (subcomponent: Client programs). Supported versions that are affected are 5.5.60 and prior, 5.6.40 and prior, 5.7.22 and prior and 8.0.11 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Client. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Client as well as unauthorized update, insert or delete access to some of MySQL Client accessible data. CVSS 3.0 Base Score 5.0 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:L/A:H). **CVE-ID:CVE-2018-3081**	https://security.netapp.com/advisory/ntap-20180726-0002/	**A-Ora-Mysql/01-08-18/210**
NA	18-07-2018	**4.9**	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Options). Supported versions that are affected are 5.5.60 and prior, 5.6.40 and prior and 5.7.22 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible	https://security.netapp.com/advisory/ntap-20180726-0002/	**A-Ora-Mysql/01-08-18/211**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			data as well as unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.0 Base Score 3.3 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:L/I:L/A:N). **CVE-ID:CVE-2018-3066**		
NA	18-07-2018	**5.5**	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.6.40 and prior, 5.7.22 and prior and 8.0.11 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 7.1 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:H). **CVE-ID:CVE-2018-3064**	https://security.netapp.com/advisory/ntap-20180726-0002/	**A-Ora-Mysql/01-08-18/212**
NA	18-07-2018	**5.5**	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.7.22 and prior and 8.0.11 and prior. Easily exploitable vulnerability allows high privileged attacker	https://security.netapp.com/advisory/ntap-20180726-0002/	**A-Ora-Mysql/01-08-18/213**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all MySQL Server accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:H). **CVE-ID:CVE-2018-3060**		
Mysql Workbench					
NA	18-07-2018	**4.3**	Vulnerability in the MySQL Workbench component of Oracle MySQL (subcomponent: Workbench: Security: Encryption). Supported versions that are affected are 6.3.10 and earlier. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Workbench. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Workbench accessible data. CVSS 3.0 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE-ID:CVE-2018-2598**	https://security.netapp.com/advisory/ntap-20180726-0002/	**A-Ora-Mysql/01-08-18/214**
One-to-one Fulfillment					

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
NA	18-07-2018	**5.8**	Vulnerability in the Oracle One-to-One Fulfillment component of Oracle E-Business Suite (subcomponent: Print Server). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6 and 12.2.7. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle One-to-One Fulfillment. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle One-to-One Fulfillment, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle One-to-One Fulfillment accessible data as well as unauthorized update, insert or delete access to some of Oracle One-to-One Fulfillment accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N). **CVE-ID:CVE-2018-2953**	NA	**A-Ora-One-t/01-08-18/215**
Order Management					
NA	18-07-2018	**4.4**	Vulnerability in the Oracle Order Management component of Oracle E-Business Suite (subcomponent: Product Diagnostic Tools). Supported versions that are affected are	NA	**A-Ora-Order/01-08-18/216**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6 and 12.2.7. Difficult to exploit vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Order Management executes to compromise Oracle Order Management. Successful attacks of this vulnerability can result in takeover of Oracle Order Management. CVSS 3.0 Base Score 7.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H). **CVE-ID:CVE-2018-2954**		
Outside In Technology					
DoS	18-07-2018	**5.8**	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). The supported version that is affected is 8.5.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Outside In Technology accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside	NA	**A-Ora-Outsi/01-08-18/217**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 7.1 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:L). **CVE-ID:CVE-2018-2992**		
DoS	18-07-2018	**5.8**	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). The supported version that is affected is 8.5.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Outside In Technology accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside	NA	**A-Ora-Outsi/01-08-18/218**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 7.1 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:L). **CVE-ID:CVE-2018-3009**		
DoS	18-07-2018	**5.8**	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). The supported version that is affected is 8.5.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Outside In Technology accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside	NA	**A-Ora-Outsi/01-08-18/219**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 7.1 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:L). **CVE-ID:CVE-2018-3010**		
DoS	18-07-2018	**5.8**	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). The supported version that is affected is 8.5.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Outside In Technology accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside	NA	**A-Ora-Outsi/01-08-18/220**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 7.1 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:L). **CVE-ID:CVE-2018-3092**		
DoS	18-07-2018	**5.8**	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). The supported version that is affected is 8.5.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Outside In Technology accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside	NA	**A-Ora-Outsi/01-08-18/221**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 7.1 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:L). **CVE-ID:CVE-2018-3093**		
DoS	18-07-2018	**5.8**	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). The supported version that is affected is 8.5.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Outside In Technology accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside	NA	**A-Ora-Outsi/01-08-18/222**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 7.1 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:L). **CVE-ID:CVE-2018-3094**		
DoS	18-07-2018	**5.8**	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). The supported version that is affected is 8.5.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Outside In Technology accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside	NA	**A-Ora-Outsi/01-08-18/223**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 7.1 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:L). **CVE-ID:CVE-2018-3095**		
DoS	18-07-2018	**5.8**	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). The supported version that is affected is 8.5.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Outside In Technology accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside	NA	**A-Ora-Outsi/01-08-18/224**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 7.1 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:L). **CVE-ID:CVE-2018-3096**		
DoS	18-07-2018	**5.8**	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). The supported version that is affected is 8.5.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Outside In Technology accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside	NA	**A-Ora-Outsi/01-08-18/225**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 7.1 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:L). **CVE-ID:CVE-2018-3097**		
DoS	18-07-2018	**5.8**	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). The supported version that is affected is 8.5.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Outside In Technology accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside	NA	**A-Ora-Outsi/01-08-18/226**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 7.1 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:L). **CVE-ID:CVE-2018-3098**		
DoS	18-07-2018	**5.8**	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). The supported version that is affected is 8.5.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Outside In Technology accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside	NA	**A-Ora-Outsi/01-08-18/227**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 7.1 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:L). **CVE-ID:CVE-2018-3099**		
DoS	18-07-2018	**5.8**	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). The supported version that is affected is 8.5.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Outside In Technology accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside	NA	**A-Ora-Outsi/01-08-18/228**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 7.1 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:L). **CVE-ID:CVE-2018-3102**		
DoS	18-07-2018	**5.8**	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). The supported version that is affected is 8.5.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Outside In Technology accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside	NA	**A-Ora-Outsi/01-08-18/229**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 7.1 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:L). **CVE-ID:CVE-2018-3103**		
DoS	18-07-2018	**5.8**	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). The supported version that is affected is 8.5.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Outside In Technology accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside	NA	**A-Ora-Outsi/01-08-18/230**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 7.1 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:L). **CVE-ID:CVE-2018-3104**		
Peoplesoft Enterprise Cs Financial Aid					
NA	18-07-2018	**4**	Vulnerability in the PeopleSoft Enterprise CS Financial Aid component of Oracle PeopleSoft Products (subcomponent: ISIR Processing). Supported versions that are affected are 9.0 and 9.2. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise CS Financial Aid. Successful attacks of this vulnerability can result in unauthorized read access to a subset of PeopleSoft Enterprise CS Financial Aid accessible data. CVSS 3.0 Base Score 2.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N). **CVE-ID:CVE-2018-3076**	NA	**A-Ora-Peopl/01-08-18/231**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
Peoplesoft Enterprise Human Capital Management Human Resources					
NA	18-07-2018	**5.8**	Vulnerability in the PeopleSoft Enterprise HCM Human Resources component of Oracle PeopleSoft Products (subcomponent: Compensation). The supported version that is affected is 9.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise HCM Human Resources. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise HCM Human Resources, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise HCM Human Resources accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise HCM Human Resources accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE-ID:CVE-2018-3068**	NA	**A-Ora-Peopl/01-08-18/232**
Peoplesoft Enterprise Peopletools					
NA	18-07-2018	**4**	Vulnerability in the PeopleSoft Enterprise PeopleTools component of Oracle PeopleSoft Products (subcomponent: PIA Search Functionality). Supported	NA	**A-Ora-Peopl/01-08-18/233**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			versions that are affected are 8.55 and 8.56. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks of this vulnerability can result in unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.0 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N). **CVE-ID:CVE-2018-2970**		
NA	18-07-2018	**4.3**	Vulnerability in the PeopleSoft Enterprise PeopleTools component of Oracle PeopleSoft Products (subcomponent: Integration Broker). Supported versions that are affected are 8.55 and 8.56. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.0 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI	NA	**A-Ora-Peopl/01-08-18/234**

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			:R/S:U/C:H/I:N/A:N). **CVE-ID:CVE-2018-2977**		
NA	18-07-2018	**5.5**	Vulnerability in the PeopleSoft Enterprise PeopleTools component of Oracle PeopleSoft Products (subcomponent: Integration Broker). Supported versions that are affected are 8.55 and 8.56. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.0 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI :N/S:U/C:L/I:L/A:N). **CVE-ID:CVE-2018-3016**	NA	**A-Ora-Peopl/01-08-18/235**
NA	18-07-2018	**5.8**	Vulnerability in the PeopleSoft Enterprise PeopleTools component of Oracle PeopleSoft Products (subcomponent: Integration Broker). Supported versions that are affected are 8.55 and 8.56. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools.	NA	**A-Ora-Peopl/01-08-18/236**

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized access to critical data or complete access to all PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.0 Base Score 7.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N). **CVE-ID:CVE-2018-2990**		
NA	18-07-2018	**5.8**	Vulnerability in the PeopleSoft Enterprise PeopleTools component of Oracle PeopleSoft Products (subcomponent: PIA Core Technology). Supported versions that are affected are 8.55 and 8.56. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data as	NA	**A-Ora-Peopl/01-08-18/237**

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE-ID:CVE-2018-2929**		
NA	18-07-2018	**5.8**	Vulnerability in the PeopleSoft Enterprise PeopleTools component of Oracle PeopleSoft Products (subcomponent: Unified Navigation). Supported versions that are affected are 8.55 and 8.56. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector:	NA	**A-Ora-Peopl/01-08-18/238**

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			(CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE-ID:CVE-2018-2919**		
NA	18-07-2018	**5.8**	Vulnerability in the PeopleSoft Enterprise PeopleTools component of Oracle PeopleSoft Products (subcomponent: Workflow). Supported versions that are affected are 8.55 and 8.56. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE-ID:CVE-2018-2985**	NA	**A-Ora-Peopl/01-08-18/239**
NA	18-07-2018	**5.8**	Vulnerability in the PeopleSoft Enterprise PeopleTools component of Oracle PeopleSoft Products (subcomponent: Workflow).	NA	**A-Ora-Peopl/01-08-18/240**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			Supported versions that are affected are 8.55 and 8.56. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE-ID:CVE-2018-2986**		
Peoplesoft Human Resource Management Systems					
NA	18-07-2018	**5**	Vulnerability in the PeopleSoft HRMS component of Oracle PeopleSoft Products (subcomponent: Candidate Gateway). The supported version that is affected is 9.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft HRMS. Successful attacks of this vulnerability can	NA	**A-Ora-Peopl/01-08-18/241**

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			result in unauthorized read access to a subset of PeopleSoft HRMS accessible data. CVSS 3.0 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE-ID:CVE-2018-3072**		
Primavera P6 Enterprise Project Portfolio Management					
NA	18-07-2018	**3.6**	Vulnerability in the Primavera P6 Enterprise Project Portfolio Management component of Oracle Construction and Engineering Suite (subcomponent: Web Access). Supported versions that are affected are 8.4, 15.x, 16.x and 17.x. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Primavera P6 Enterprise Project Portfolio Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Primavera P6 Enterprise Project Portfolio Management, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Primavera P6 Enterprise Project Portfolio Management accessible data as well as unauthorized read access to a subset of Primavera P6 Enterprise Project Portfolio Management accessible data.	NA	**A-Ora-Prima/01-08-18/242**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			CVSS 3.0 Base Score 4.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:C/C:L/I:L/A:N). **CVE-ID:CVE-2018-2962**		
NA	18-07-2018	**4**	Vulnerability in the Primavera P6 Enterprise Project Portfolio Management component of Oracle Construction and Engineering Suite (subcomponent: Web Access). Supported versions that are affected are 8.4, 15.x and 16.x. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Primavera P6 Enterprise Project Portfolio Management. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Primavera P6 Enterprise Project Portfolio Management accessible data. CVSS 3.0 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N). **CVE-ID:CVE-2018-2963**	NA	**A-Ora-Prima/01-08-18/243**
NA	18-07-2018	**5.8**	Vulnerability in the Primavera P6 Enterprise Project Portfolio Management component of Oracle Construction and Engineering Suite (subcomponent: Web Access). Supported versions that are affected are 8.4, 15.x, 16.x and 17.x. Easily exploitable vulnerability allows unauthenticated attacker with network access	NA	**A-Ora-Prima/01-08-18/244**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			via HTTP to compromise Primavera P6 Enterprise Project Portfolio Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Primavera P6 Enterprise Project Portfolio Management, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Primavera P6 Enterprise Project Portfolio Management accessible data as well as unauthorized read access to a subset of Primavera P6 Enterprise Project Portfolio Management accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE-ID:CVE-2018-2960**		
NA	18-07-2018	**5.8**	Vulnerability in the Primavera P6 Enterprise Project Portfolio Management component of Oracle Construction and Engineering Suite (subcomponent: Web Access). Supported versions that are affected are 8.4, 15.x, 16.x and 17.x. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Primavera P6 Enterprise Project Portfolio Management. Successful attacks require	NA	**A-Ora-Prima/01-08-18/245**

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			human interaction from a person other than the attacker and while the vulnerability is in Primavera P6 Enterprise Project Portfolio Management, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Primavera P6 Enterprise Project Portfolio Management accessible data as well as unauthorized read access to a subset of Primavera P6 Enterprise Project Portfolio Management accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE-ID:CVE-2018-2961**		
Primavera Unifier					
NA	18-07-2018	**4**	Vulnerability in the Primavera Unifier component of Oracle Construction and Engineering Suite (subcomponent: Core). The supported version that is affected is 16.x. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Primavera Unifier. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Primavera Unifier accessible data. CVSS 3.0 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI	NA	**A-Ora-Prima/01-08-18/246**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			:N/S:U/C:L/I:N/A:N). **CVE-ID:CVE-2018-2969**		
NA	18-07-2018	**4.3**	Vulnerability in the Primavera Unifier component of Oracle Construction and Engineering Suite (subcomponent: Core). Supported versions that are affected are 16.x, 17.x and 18.x. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Primavera Unifier. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Primavera Unifier, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Primavera Unifier accessible data. CVSS 3.0 Base Score 7.4 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI :R/S:C/C:N/I:H/A:N). **CVE-ID:CVE-2018-2966**	NA	**A-Ora-Prima/01-08-18/247**
NA	18-07-2018	**4.3**	Vulnerability in the Primavera Unifier component of Oracle Construction and Engineering Suite (subcomponent: Core). Supported versions that are affected are 16.x, 17.x and 18.x. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Primavera Unifier. Successful attacks require human	NA	**A-Ora-Prima/01-08-18/248**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Primavera Unifier accessible data. CVSS 3.0 Base Score 6.5 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N). **CVE-ID:CVE-2018-2968**		
NA	18-07-2018	**5.8**	Vulnerability in the Primavera Unifier component of Oracle Construction and Engineering Suite (subcomponent: Core). The supported version that is affected is 16.x. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Primavera Unifier. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Primavera Unifier, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Primavera Unifier accessible data as well as unauthorized read access to a subset of Primavera Unifier accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	NA	**A-Ora-Prima/01-08-18/249**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			CVE-ID:CVE-2018-2965		
Retail Bulk Data Integration					
NA	18-07-2018	**5.8**	Vulnerability in the Oracle Retail Bulk Data Integration component of Oracle Retail Applications (subcomponent: BDI Job Scheduler). The supported version that is affected is 16.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Retail Bulk Data Integration. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Retail Bulk Data Integration, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Retail Bulk Data Integration accessible data as well as unauthorized read access to a subset of Oracle Retail Bulk Data Integration accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE-ID:CVE-2018-2891**	NA	**A-Ora-Retai/01-08-18/250**
Retail Customer Management And Segmentation Foundation					
DoS	18-07-2018	**5.5**	Vulnerability in the Oracle Retail Customer Management and Segmentation Foundation component of Oracle Retail Applications (subcomponent: Internal Operations).	NA	**A-Ora-Retai/01-08-18/251**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			Supported versions that are affected are 16.x and 17.x. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Retail Customer Management and Segmentation Foundation. While the vulnerability is in Oracle Retail Customer Management and Segmentation Foundation, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Retail Customer Management and Segmentation Foundation accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Retail Customer Management and Segmentation Foundation. CVSS 3.0 Base Score 6.4 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:N/I:L/A:L). **CVE-ID:CVE-2018-3053**		
Scripting					
NA	18-07-2018	**5.8**	Vulnerability in the Oracle Scripting component of Oracle E-Business Suite (subcomponent: Script Author). Supported versions that are affected are 12.1.1, 12.1.2 and 12.1.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise	NA	**A-Ora-Scrip/01-08-18/252**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			Oracle Scripting. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Scripting, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Scripting accessible data as well as unauthorized update, insert or delete access to some of Oracle Scripting accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N). **CVE-ID:CVE-2018-2997**		
Siebel Ui Framework					
NA	18-07-2018	**4.3**	Vulnerability in the Siebel UI Framework component of Oracle Siebel CRM (subcomponent: UIF Open UI). The supported version that is affected is 18.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Siebel UI Framework. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Siebel UI Framework accessible data. CVSS 3.0 Base Score 4.3 (Integrity impacts). CVSS	NA	**A-Ora-Siebe/01-08-18/253**

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N). **CVE-ID:CVE-2018-2959**		
Soa Suite					
NA	18-07-2018	**4**	Vulnerability in the Oracle SOA Suite component of Oracle Fusion Middleware (subcomponent: Health Care FastPath). Supported versions that are affected are 11.1.1.7.0, 11.1.1.9.0, 12.1.3.0.0, 12.2.1.2.0 and 12.2.1.3.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle SOA Suite. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle SOA Suite accessible data. CVSS 3.0 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N). **CVE-ID:CVE-2018-3105**	NA	**A-Ora-Soa/01-08-18/254**
Solaris Cluster					
NA	18-07-2018	**7.5**	Vulnerability in the Solaris Cluster component of Oracle Sun Systems Products Suite (subcomponent: NAS device addition). Supported versions that are affected are 3.3 and 4.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via RPC to compromise Solaris Cluster. Successful attacks of this vulnerability can result in takeover of Solaris Cluster. CVSS 3.0 Base Score 9.8 (Confidentiality, Integrity and	NA	**A-Ora-Solar/01-08-18/255**

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H). **CVE-ID:CVE-2018-2930**		
Trade Management					
NA	18-07-2018	**5.8**	Vulnerability in the Oracle Trade Management component of Oracle E-Business Suite (subcomponent: User Interface). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6 and 12.2.7. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Trade Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Trade Management, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Trade Management accessible data as well as unauthorized update, insert or delete access to some of Oracle Trade Management accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N). **CVE-ID:CVE-2018-2991**	NA	**A-Ora-Trade/01-08-18/256**
NA	18-07-2018	**5.8**	Vulnerability in the Oracle Trade Management	NA	**A-Ora-Trade/01**

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			component of Oracle E-Business Suite (subcomponent: User Interface). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6 and 12.2.7. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Trade Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Trade Management, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Trade Management accessible data as well as unauthorized update, insert or delete access to some of Oracle Trade Management accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N). **CVE-ID:CVE-2018-3012**		**-08-18/257**
Tuxedo					
NA	18-07-2018	**5**	Vulnerability in the Oracle Tuxedo component of Oracle Fusion Middleware (subcomponent: Core). Supported versions that are affected are 12.1.1, 12.1.3 and 12.2.2. Easily exploitable vulnerability allows unauthenticated attacker with	NA	**A-Ora-Tuxed/01-08-18/258**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			network access via Jolt to compromise Oracle Tuxedo. While the vulnerability is in Oracle Tuxedo, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Tuxedo accessible data. CVSS 3.0 Base Score 8.6 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N). **CVE-ID:CVE-2018-3007**		
Vm Virtualbox					
NA	18-07-2018	**3.3**	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). The supported version that is affected is Prior to 5.2.16. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox and unauthorized read access to a subset of Oracle VM VirtualBox	NA	**A-Ora-Vm/01-08-18/259**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			accessible data. CVSS 3.0 Base Score 7.1 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:C/C:L/I:N/A:H). **CVE-ID:CVE-2018-3055**		
NA	18-07-2018	**4.4**	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). The supported version that is affected is Prior to 5.2.16. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 8.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H). **CVE-ID:CVE-2018-3086**	NA	**A-Ora-Vm/01-08-18/260**
NA	18-07-2018	**4.4**	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). The supported version that is affected is Prior to 5.2.16. Easily exploitable vulnerability allows unauthenticated	NA	**A-Ora-Vm/01-08-18/261**

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 8.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H). **CVE-ID:CVE-2018-3087**		
NA	18-07-2018	**4.4**	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). The supported version that is affected is Prior to 5.2.16. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base	NA	**A-Ora-Vm/01-08-18/262**

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			Score 8.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H). **CVE-ID:CVE-2018-3088**		
NA	18-07-2018	**4.4**	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). The supported version that is affected is Prior to 5.2.16. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 8.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H). **CVE-ID:CVE-2018-3089**	NA	**A-Ora-Vm/01-08-18/263**
NA	18-07-2018	**4.4**	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). The supported version that is affected is Prior to 5.2.16. Easily exploitable vulnerability allows unauthenticated attacker with logon to the	NA	**A-Ora-Vm/01-08-18/264**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 8.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H). **CVE-ID:CVE-2018-3090**		
NA	18-07-2018	**4.4**	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). The supported version that is affected is Prior to 5.2.16. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle VM	NA	**A-Ora-Vm/01-08-18/265**

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			VirtualBox accessible data as well as unauthorized read access to a subset of Oracle VM VirtualBox accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox. CVSS 3.0 Base Score 8.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:C/C:L/I:H/A:H). **CVE-ID:CVE-2018-3085**		
Webcenter Portal					
NA	18-07-2018	**5**	Vulnerability in the Oracle WebCenter Portal component of Oracle Fusion Middleware (subcomponent: Portlet Services). Supported versions that are affected are 11.1.1.9.0, 12.2.1.2.0 and 12.2.1.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebCenter Portal. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle WebCenter Portal accessible data. CVSS 3.0 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE-ID:CVE-2018-3101**	NA	**A-Ora-Webce/01-08-18/266**
Weblogic Server					
DoS	18-07-2018	**5.8**	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: JSF). Supported versions that are affected are 10.3.6.0, 12.1.3.0,	NA	**A-Ora-Weblo/01-08-18/267**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			12.2.1.2 and 12.2.1.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle WebLogic Server accessible data as well as unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle WebLogic Server. CVSS 3.0 Base Score 8.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:L). **CVE-ID:CVE-2018-2935**		
NA	18-07-2018	**5.5**	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: SAML). Supported versions that are affected are 10.3.6.0, 12.1.3.0, 12.2.1.2 and 12.2.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some	NA	**A-Ora-Weblo/01-08-18/268**

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			of Oracle WebLogic Server accessible data as well as unauthorized read access to a subset of Oracle WebLogic Server accessible data. CVSS 3.0 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N). **CVE-ID:CVE-2018-2998**		
NA	18-07-2018	**5.8**	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: Console). Supported versions that are affected are 10.3.6.0, 12.1.3.0, 12.2.1.2 and 12.2.1.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle WebLogic Server, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle WebLogic Server accessible data as well as unauthorized read access to a subset of Oracle WebLogic Server accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	NA	**A-Ora-Weblo/01-08-18/269**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			CVE-ID:CVE-2018-2987		
NA	18-07-2018	**7.5**	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: WLS Core Components). Supported versions that are affected are 10.3.6.0, 12.1.3.0, 12.2.1.2 and 12.2.1.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3 to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.0 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H). **CVE-ID:CVE-2018-2893**	NA	**A-Ora-Weblo/01-08-18/270**
NA	18-07-2018	**7.5**	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: WLS - Web Services). Supported versions that are affected are 10.3.6.0, 12.1.3.0, 12.2.1.2 and 12.2.1.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.0 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	NA	**A-Ora-Weblo/01-08-18/271**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			CVE-ID:CVE-2018-2894		
Orderbook Presale Token Project					
Orderbook Presale Token					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for Orderbook Presale Token (OBP), an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13676**	https://github.com/BlockChainsSecurity/EtherTokens/tree/master/PresaleToken, https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md	**A-Ord-Order/01-08-18/272**
Otakutoken Project					
Otakutoken					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for OTAKUToken, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13755**	https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md, https://github.com/BlockChainsSecurity/EtherTokens/tree/master/OTAKUToken	**A-Ota-Otaku/01-08-18/273**
Pelocointoken Project					
Pelocointoken					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for PELOCoinToken, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13738**	https://github.com/BlockChainsSecurity/EtherTokens/tree/master/PELOCoinToken, https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%2	**A-Pel-Peloc/01-08-18/274**

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
				0integer%20overflow.md	
Play2livepromo Project					
Play2livepromo					
Overflow	09-07-2018	**5**	The mintTokens function of a smart contract implementation for Play2LivePromo, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13698**	https://github.com/BlockChainsSecurity/EtherTokens/tree/master/Play2LivePromo, https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md	**A-Pla-Play2/01-08-18/275**
Pmet Project					
Pmet					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for PMET, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13712**	https://github.com/BlockChainsSecurity/EtherTokens/tree/master/PMET, https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md	**A-Pme-Pmet/01-08-18/276**
Pmhtoken Project					
Pmhtoken					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for PMHToken, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13705**	https://github.com/BlockChainsSecurity/EtherTokens/tree/master/PMHToken, https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GE	**A-Pmh-Pmhto/01-08-18/277**

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
				MCHAIN/mint%20integer%20overflow.md	
Projectj Project					
Projectj					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for ProjectJ, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13733**	https://github.com/BlockChainsSecurity/EtherTokens/tree/master/ProjectJ, https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md	**A-Pro-Proje/01-08-18/278**
Rckt Coin Project					
Rckt Coin					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for RCKT_Coin, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13775**	https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md, https://github.com/BlockChainsSecurity/EtherTokens/tree/master/RCKT_Coin	**A-Rck-Rckt/01-08-18/279**
Redticket Project					
Redticket					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for RedTicket, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13696**	https://github.com/BlockChainsSecurity/EtherTokens/tree/master/RedTicket, https://github.com/BlockChainsSecurity/EtherTokens	**A-Red-Redti/01-08-18/280**

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
				/blob/master/GEMCHAIN/mint%20integer%20overflow.md	
Richiumtoken Project					
Richiumtoken					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for RichiumToken, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13750**	https://github.com/BlockChainsSecurity/EtherTokens/tree/master/RichiumToken, https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md	**A-Ric-Richi/01-08-18/281**
Riptidecoin Project					
Riptidecoin					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for RiptideCoin (RIPT), an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13732**	https://github.com/BlockChainsSecurity/EtherTokens/tree/master/RiptideCoin, https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md	**A-Rip-Ripti/01-08-18/282**
Robotbtc Project					
Robotbtc					

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for RobotBTC, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13697**	https://github.com/BlockChainsSecurity/EtherTokens/tree/master/RobotBTC, https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md	**A-Rob-Robot/01-08-18/283**
Rocket Coin Project					
Rocket Coin					
Overflow	12-07-2018	**5**	An integer overflow vulnerability exists in the function multiTransfer of Rocket Coin (XRC), an Ethereum token smart contract. An attacker could use it to set any user's balance. **CVE-ID:CVE-2018-13836**	https://github.com/VenusADLab/EtherTokens/tree/master/Rocket%20Coin%28XRC%29, https://github.com/VenusADLab/EtherTokens/blob/master/SHARKTECH/SHARKTECH.md	**A-Roc-Rocke/01-08-18/284**
Rrtoken Project					
Rrtoken					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for RRToken, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13777**	https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md, https://github.com/BlockChainsSecurity/EtherTokens/tree/master/RRToken	**A-Rrt-Rrtok/01-08-18/285**
Rtokenmain Project					

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
Rtokenmain					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for R Time Token v3 (RS) (Contract Name: RTokenMain), an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13691**	https://github.com/BlockChainsSecurity/EtherTokens/tree/master/RTokenMain, https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md	**A-Rto-Rtoke/01-08-18/286**
Servviziotoken Project					
Servviziotoken					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for SERVVIZIOToken, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13723**	https://github.com/BlockChainsSecurity/EtherTokens/tree/master/SERVVIZIOToken, https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md	**A-Ser-Servv/01-08-18/287**
Sexhdsolo Project					
Sexhdsolo					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for sexhdsolo, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13716**	https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md, https://github.com/BlockChainsSecurity/EtherTokens/tree/master/sexhdsolo	**A-Sex-Sexhd/01-08-18/288**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
Sharktech Project					
Sharktech					
Overflow	12-07-2018	**5**	An integer overflow vulnerability exists in the function batchTransfer of SHARKTECH (SKT), an Ethereum token smart contract. An attacker could use it to set any user's balance. **CVE-ID:CVE-2018-14001**	https://github.com/VenusADLab/EtherTokens/blob/master/SHARKTECH/SHARKTECH.md	**A-Sha-Shark/01-08-18/289**
Soscoin Project					
Soscoin					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for SOSCoin, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13681**	https://github.com/BlockChainsSecurity/EtherTokens/tree/master/SOSCoin, https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md	**A-Sos-Sosco/01-08-18/290**
Stctoken Project					
Stctoken					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for STCToken, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13745**	https://github.com/BlockChainsSecurity/EtherTokens/tree/master/STCToken, https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md	**A-Stc-Stcto/01-08-18/291**
Superenergy Project					
Superenergy					

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for SuperEnergy (SEC), an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13743**	https://github.com/BlockChainsSecurity/EtherTokens/tree/master/SEC, https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md	**A-Sup-Super/01-08-18/292**
Theflashtoken Project					
Theflashtoken					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for TheFlashToken, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13772**	https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md, https://github.com/BlockChainsSecurity/EtherTokens/tree/master/TheFlashToken	**A-The-Thefl/01-08-18/293**
Thread Project					
Thread					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for Thread, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13752**	https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md, https://github.com/BlockChainsSecurity/EtherTokens/tree/master/Thread	**A-Thr-Threa/01-08-18/294**
Tickets Project					
Tickets					

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for tickets (TKT), an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13742**	https://github.com/BlockChainsSecurity/EtherTokens/tree/master/tickets, https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md	**A-Tic-Ticke/01-08-18/295**
Tokenmachu Project					
Tokenmachu					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for TokenMACHU, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13731**	https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md, https://github.com/BlockChainsSecurity/EtherTokens/tree/master/TokenMACHU	**A-Tok-Token/01-08-18/296**
Tradesman Project					
Tradesman					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for Tradesman, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13713**	https://github.com/BlockChainsSecurity/EtherTokens/tree/master/Tradesman, https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md	**A-Tra-Trade/01-08-18/297**
Tube Project					

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
Tube					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for Tube, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13709**	https://github.com/BlockChainsSecurity/EtherTokens/tree/master/Tube, https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md	**A-Tub-Tube/01-08-18/298**
Ublasti Project					
Ublasti					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for Ublasti, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13763**	https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md, https://github.com/BlockChainsSecurity/EtherTokens/tree/master/Ublasti	**A-Ubl-Ublas/01-08-18/299**
Ultimatecoin Project					
Ultimatecoin					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for UltimateCoin, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13770**	https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md, https://github.com/BlockChainsSecurity/EtherTokens/tree/master/UltimateCoin	**A-Ult-Ultim/01-08-18/300**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
Utbtokentest Project					
Utbtokentest					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for UTBTokenTest, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13667**	https://github.com/BlockChainsSecurity/EtherTokens/tree/master/UTBTokenTest, https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md	**A-Utb-Utbto/01-08-18/301**
Vanminhcoin Project					
Vanminhcoin					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for VanMinhCoin, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13747**	https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md, https://github.com/BlockChainsSecurity/EtherTokens/tree/master/VanMinhCoin	**A-Van-Vanmi/01-08-18/302**
Vitemoneycoin Project					
Vitemoneycoin					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for ViteMoneyCoin, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13682**	https://github.com/BlockChainsSecurity/EtherTokens/tree/master/ViteMoneyCoin, https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overf	**A-Vit-Vitem/01-08-18/303**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
				low.md	
Vornoxcointoken Project					
Vornoxcointoken					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for Vornox (VRX) (Contract Name: VornoxCoinToken), an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13685**	https://github.com/BlockChainsSecurity/EtherTokens/tree/master/CoinToken, https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md	**A-Vor-Vorno/01-08-18/304**
Wemediachain Project					
Wemediachain					
Overflow	12-07-2018	**5**	An integer overflow vulnerability exists in the function batchTransfer of WeMediaChain (WMC), an Ethereum token smart contract. An attacker could use it to set any user's balance. **CVE-ID:CVE-2018-14003**	https://github.com/VenusADLab/EtherTokens/tree/master/WeMediaChain%28WMC%29, https://github.com/VenusADLab/EtherTokens/blob/master/SHARKTECH/SHARKTECH.md	**A-Wem-Wemed/01-08-18/305**
Worldopctionchain Project					
Worldopctionchain					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for WorldOpctionChain, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13662**	https://github.com/BlockChainsSecurity/EtherTokens/tree/master/WorldOpctionChain, https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%2	**A-Wor-World/01-08-18/306**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
				0integer%20overflow.md	
Yambyo Project					
Yambyo					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for YAMBYO, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13675**	https://github.com/BlockChainsSecurity/EtherTokens/tree/master/YAMBYO, https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md	**A-Yam-Yamby/01-08-18/307**
Ylctoken Project					
Ylctoken					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for YLCToken, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13779**	https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md, https://github.com/BlockChainsSecurity/EtherTokens/tree/master/YLCToken	**A-Ylc-Ylcto/01-08-18/308**
Yss Project					
YSS					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for YSS, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13707**	https://github.com/BlockChainsSecurity/EtherTokens/tree/master/YSS, https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%2	**A-Yss-YSS/01-08-18/309**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
				0integer%20overflow.md	
Yumerium Project					
Yumerium					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for Yumerium, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13762**	https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md https://github.com/BlockChainsSecurity/EtherTokens/tree/master/Yumerium	**A-Yum-Yumer/01-08-18/310**
Zip Project					
ZIP					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for ZIP, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13684**	https://github.com/BlockChainsSecurity/EtherTokens/tree/master/ZIP, https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md	**A-Zip-ZIP/01-08-18/311**
Zpecoin Project					
Zpecoin					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for ZPEcoin, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13679**	https://github.com/BlockChainsSecurity/EtherTokens/tree/master/ZPEcoin, https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%2	**A-Zpe-Zpeco/01-08-18/312**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
				0integer%20overflow.md	
Ztoken Project					
Ztoken					
Overflow	09-07-2018	**5**	The mintToken function of a smart contract implementation for ZToken, an Ethereum token, has an integer overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. **CVE-ID:CVE-2018-13768**	https://github.com/BlockChainsSecurity/EtherTokens/blob/master/GEMCHAIN/mint%20integer%20overflow.md, https://github.com/BlockChainsSecurity/EtherTokens/tree/master/ZToken	**A-Zto-Ztoke/01-08-18/313**
Hardware					
ARM,Intel					
Atom C,Atom E,Atom X3,Atom Z,Celeron J,Celeron N,Core I3,Core I5,Core I7,Core M,Core M3,Core M5,Core M7,Cortex-a,Cortex-r,Pentium J,Pentium N,Xeon,Xeon Bronze,Xeon E3					
Overflow Gain Information	10-07-2018	**4.7**	Systems with microprocessors utilizing speculative execution and branch prediction may allow unauthorized disclosure of information to an attacker with local user access via a speculative buffer overflow and side-channel analysis. **CVE-ID:CVE-2018-3693**	https://www.suse.com/support/kb/doc/?id7023075, https://thehackernews.com/2018/07/intel-spectre-vulnerability.html, https://01.org/security/advisories/intel-oss-10002	**H-ARM-Atom/01-08-18/314**
Operating System (OS)					
Oracle					
Solaris					
DoS	18-07-2018	**4.3**	Vulnerability in the Solaris component of Oracle Sun Systems Products Suite (subcomponent: Kernel). Supported versions that are affected are 10 and 11.2. Difficult to exploit	NA	**O-Ora-Solar/01-08-18/315**

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			vulnerability allows unauthenticated attacker with network access via DHCP to compromise Solaris. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Solaris. CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE-ID:CVE-2018-2901**		
NA	18-07-2018	**4.9**	Vulnerability in the Solaris component of Oracle Sun Systems Products Suite (subcomponent: Kernel). Supported versions that are affected are 10 and 11.3. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Solaris executes to compromise Solaris. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Solaris accessible data. CVSS 3.0 Base Score 4.4 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N). **CVE-ID:CVE-2018-2903**	NA	**O-Ora-Solar/01-08-18/316**
NA	18-07-2018	**6.8**	Vulnerability in the Solaris component of Oracle Sun Systems Products Suite (subcomponent: Kernel). The supported version that is affected is 11.3. Easily exploitable vulnerability allows low privileged attacker	NA	**O-Ora-Solar/01-08-18/317**

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			with network access via RPC to compromise Solaris. While the vulnerability is in Solaris, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Solaris. CVSS 3.0 Base Score 7.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H). **CVE-ID:CVE-2018-2908**		
NA	18-07-2018	**7.2**	Vulnerability in the Solaris component of Oracle Sun Systems Products Suite (subcomponent: Availability Suite Service). Supported versions that are affected are 10 and 11.3. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Solaris executes to compromise Solaris. Successful attacks of this vulnerability can result in takeover of Solaris. CVSS 3.0 Base Score 7.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H). **CVE-ID:CVE-2018-2892**	NA	**O-Ora-Solar/01-08-18/318**
NA	18-07-2018	**8**	Vulnerability in the Solaris component of Oracle Sun Systems Products Suite (subcomponent: NVIDIA-GFX Kernel driver). The supported version that is affected is 11.3. Easily exploitable vulnerability	NA	**O-Ora-Solar/01-08-18/319**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			allows low privileged attacker with network access via ISCSI to compromise Solaris. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Solaris as well as unauthorized update, insert or delete access to some of Solaris accessible data and unauthorized read access to a subset of Solaris accessible data. CVSS 3.0 Base Score 7.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:H). **CVE-ID:CVE-2018-2926**		
NA	18-07-2018	**8.8**	Vulnerability in the Solaris component of Oracle Sun Systems Products Suite (subcomponent: RAD). The supported version that is affected is 11.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Solaris. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Solaris accessible data as well as unauthorized access to critical data or complete access to all Solaris accessible data. CVSS 3.0 Base Score 8.1	NA	**O-Ora-Solar/01-08-18/320**

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			(Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N). **CVE-ID:CVE-2018-2928**		