NOUPC	ional Critica			CVE Repor	t	Protection		
Vulnerability	Scoring Scale	: 3-10	01	l Jul-31 Jul	12018		Vol.	05 No.14
Type(s)	Publish Date	CVSS	Desci	ription & CVI	E ID	Reference/	'Patch	NCIIPC ID
Application								
Ablgenesistok	en Project							
Ablgenesistoke	T							
Overflow	09-07-2018	5	smart con for ABI Ethereum overflow to of the contained balance of any value.	Foken function function function fract implements. Genesis Token to the following the following fract in the following fract f	entation in, an integer e owner set the user to	https://gith m/BlockCha urity/Ether? /tree/maste GenesisToke https://gith m/BlockCha urity/Ether? /blob/maste MCHAIN/mi Ointeger%20 low.md	ninsSec Fokens er/ABL en, ub.co ninsSec Fokens er/GE int%2	A-Abl- Ablge/01- 08-18/1
Anovabace Pro	oject							
Anovabace								
Overflow Appletoken Pr	09-07-2018	5	smart con for Anova token, has that allow contract t an arbitra	Token function fract implements an integer of the owner of set the balary user to an VE-2018-137	entation chereum overflow of the lance of y value.	https://gith m/BlockCha urity/Ether' /tree/maste vaBace, https://gith m/BlockCha urity/Ether' /blob/maste MCHAIN/mi Ointeger%26 low.md	insSec Γokens er/Ano ub.co insSec Γokens er/GE int%2	A-Ano- Anova/01 -08-18/2
Appletoken Pi	oject							
Overflow	09-07-2018	5	smart con for Apple token, has that allow	Token functi tract impleme Token, an Et an integer o es the owner o set the bal	entation chereum overflow of the	https://gith m/BlockCha urity/Ether' /blob/maste MCHAIN/mi 0integer%2	ninsSec Fokens er/GE int%2	A-App- Apple/01- 08-18/3
CV Scoring Scale (C	vss)	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type	(s): CSRF-Cross Site CSS- Cross Site Script		orgery; Dir. T	avDirectory Tr	aversal; Do	S-Denial of Serv	ice; NA- No	ot Applicable;

			an arbitrary user to any value. CVE-ID:CVE-2018-13776	low.md, https://github.co m/BlockChainsSec urity/EtherTokens /tree/master/App leToken	
Azttoken Projec	ct				
Azttoken				<u>, </u>	
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.co m/BlockChainsSec urity/EtherTokens /tree/master/AZT Token, https://github.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 0integer%20overf low.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.co m/BlockChainsSec urity/EtherTokens /tree/master/BCa aS, https://github.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 Ointeger%20overf low.md	A-Bca- Bcaas/01- 08-18/5
Bigcadvancedto					
Bigcadvancedto l	ken 09-07-2018	5	The mintToken function of a smart contract implementation for BIGCAdvancedToken, an Ethereum token, has an integer	https://github.co m/BlockChainsSec urity/EtherTokens /blob/master/GE	A-Big- Bigca/01- 08-18/6
CV Scoring Scale (CVS	SS)	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
J (-)			overflow that allows the owner of the contract to set the balance of an arbitrary user to any value. CVE-ID:CVE-2018-13759	0integer%20overf	
				m/BlockChainsSec urity/EtherTokens /tree/master/BIG CAdvancedToken	
Biqutoken Pro	ject			Gravancea ronen	
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	m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 Ointeger%20overf	A-Biq- Biqut/01- 08-18/7
				https://github.co m/BlockChainsSec urity/EtherTokens /tree/master/Biq uToken	
Bitedutoken P	roject				
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	m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 0integer%20overf	A-Bit- Bited/01- 08-18/8
Bitstarti Projec	ct				
Bitstarti Overflow	09-07-2018	5	The mintToken function of a	https://github.co	A-Bit-
Overnow	09-07-2018	3	smart contract implementation	1 // 0	Bitst/01-
CV Scoring Scale (CV		3-4	4-5 5-6 6-7	7-8 8-9	9-10

Vulnerability Type(s)	Publish Date	cvss	Descrip	otion & CVE	: ID	Reference/	Patch	NCIIPC ID
			for Bitstar token, has a that allows contract to an arbitrary CVE-ID:CVE	n integer o the owner set the bal user to an	of the ance of y value.	urity/Ether?/blob/maste/MCHAIN/mi/Ointeger%20low.md, https://gith/m/BlockCha	er/GE nt%2 Doverf ub.co	08-18/9
						urity/Ether // /tree/maste	Γokens	
Bpstoken Proj	ect							
Bpstoken							1	
Overflow	09-07-2018	5	The mintTo smart contract to token, has a that allows contract to an arbitrary CVE-ID:CVE	act impleme sen, an Et an integer o the owner set the bal vuser to an	entation hereum verflow of the ance of y value.	https://githem/BlockChaurity/EtherToken, https://githem/BlockChaurity/EtherToken/BlockChaurity/EtherToken/Blob/mastem/Blob/mas	insSec Tokens r/Bps ub.co insSec Tokens er/GE nt%2	A-Bps- Bpsto/01- 08-18/10
Bsctoken Proje	ect							
Bsctoken Overflow	09-07-2018	5	The mintTo smart contract to token, has a that allows contract to an arbitrary CVE-ID:CVE	act impleme ken, an Et an integer o the owner set the bal vuser to an	entation hereum verflow of the ance of y value.	https://githm/BlockChaurity/EtherToken, https://githm/BlockChaurity/EtherToklob/maste/blob/maste/MCHAIN/mi0integer%20	insSec Fokens r/BSC ub.co insSec Fokens er/GE nt%2	A-Bsc- Bscto/01- 08-18/11
Btpcoin Project	t							
Btpcoin								
CV Scoring Scale (C)	ucc)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

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

Vulnerability Type(s)	Publish Date	cvss	Descrij	ption & CVE	EID	Reference	e/Patch	NCIIPC ID
Overflow	09-07-2018	5	The mintTo smart contr for BTPCo token, has a that allows contract to an arbitrary CVE-ID:CVE	act impleme in, an Et an integer o the owner set the bal vuser to an	entation hereum verflow of the ance of y value.	https://git m/BlockCl urity/Ethe /tree/mas Coin, https://git m/BlockCl urity/Ethe /blob/mas MCHAIN/r Ointeger% low.md	hub.co nainsSec rTokens ter/BTP hub.co nainsSec rTokens ter/GE nint%2	A-Btp- Btpco/01- 08-18/12
Buytoken Proj	ect							
Buytoken								
Overflow	09-07-2018	5	The mintTo smart control for Order Name: Ethereum to overflow the of the conbalance of a any value. CVE-ID:CVE	act impleme (ETH) (C BuyToken), oken, has an at allows the ntract to s	entation Contract an integer e owner set the user to	https://git m/BlockCl urity/Ethe /tree/mas Token, https://git m/BlockCl urity/Ethe /blob/mas MCHAIN/r Ointeger% low.md	hub.co hainsSec rTokens ter/Buy hub.co hainsSec rTokens ter/GE nint%2	A-Buy- Buyto/01 -08- 18/13
Cartoken Proje	ect							
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://git m/BlockCl urity/Ethe /blob/mas MCHAIN/r Ointeger% low.md, https://git m/BlockCl	nainsSec rTokens ster/GE nint%2 20overf	A-Car- Carto/01- 08-18/14	
Cerb Coin Proj	ect					urity/Ethe /tree/mas Token	rTokens	
		3-4	4-5	5-6	6-7	7-8	8-9	9-10
CV Scoring Scale (C Vulnerability Type Sql-SQL Injection; X	(s): CSRF-Cross Site	_	orgery; Dir. Tra	vDirectory Tr	aversal; Do	S-Denial of Ser	vice; NA- No	ot Applicable;

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.co m/BlockChainsSec urity/EtherTokens /tree/master/CER B_Coin, https://github.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 0integer%20overf low.md	A-Cer- Cerb/01- 08-18/15
Cgctoken Proje	ect				
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.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 0integer%20overf low.md, https://github.co m/BlockChainsSec urity/EtherTokens /tree/master/CGC Token	A-Cgc- Cgcto/01- 08-18/16
9	ndation Projec	t			
Cherrycoinfour				I	
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.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 Ointeger%20overf low.md, https://github.co m/BlockChainsSec urity/EtherTokens /tree/master/Che rryCoinFoundatio n	A-Che- Cherr/01- 08-18/17
CV Scoring Scale (C	VSS)	3-4	4-5 5-6 6-7	7-8 8-9	9-10
			4-5 5-6 6-7 orgery; Dir. TravDirectory Traversal; Do		

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Reference/Patch	NCIIPC ID
Cjxtoken Proje	ct				
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.co m/BlockChainsSec urity/EtherTokens /tree/master/CJX Token, https://github.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 Ointeger%20overf low.md	A-Cjx- Cjxto/01- 08-18/18
Cm Project					
СМ					
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.co m/BlockChainsSec urity/EtherTokens /tree/master/CM, https://github.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 Ointeger%20overf low.md	A-Cm- CM/01- 08-18/19
Coinquer Proje	ect				
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.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 Ointeger%20overf low.md, https://github.co m/BlockChainsSec urity/EtherTokens /tree/master/Coi nquer	A-Coi- Coinq/01- 08-18/20
CV Scoring Scale (CV	/SS)	3-4	4-5 5-6 6-7	7-8 8-9	9-10
		Request F	orgery; Dir. TravDirectory Traversal; Do	oS-Denial of Service; NA- No	ot Applicable;

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Reference/Patch	NCIIPC ID
Combilladvanc	edtoken Proje	ct			
Combilladvanc	edtoken				
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.co m/BlockChainsSec urity/EtherTokens /tree/master/Co mBillAdvancedTo ken, https://github.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 Ointeger%20overf low.md	A-Com- Combi/01 -08- 18/21
Cornerstone Pi	roject			,	
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.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 Ointeger%20overf low.md, https://github.co m/BlockChainsSec urity/EtherTokens /tree/master/Cor nerstone	A-Cor- Corne/01 -08- 18/22
Crowdnext Pro	ject				
Crowdnext				1.	
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.co m/BlockChainsSec urity/EtherTokens /tree/master/Cro wdnext, https://github.co m/BlockChainsSec urity/EtherTokens /blob/master/GE	A-Cro- Crowd/01 -08- 18/23
	vaa:	3-4	4-5 5-6 6-7	7-8 8-9	9-10
CV Scoring Scale (CVSS)		3.	0-7		, 10

Cryptosistoken F Cryptosistoken Overflow	Project 09-07-2018	5	The mintToken function of a smart contract implementation	MCHAIN/mint%2 Ointeger%20overf low.md https://github.co	
Cryptosistoken		5		_ ,, _	
	09-07-2018	5		_ ,, _	
Overflow	09-07-2018	5		_ ,, _	
			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	m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 Ointeger%20overf low.md, https://github.co m/BlockChainsSec urity/EtherTokens /tree/master/Cry ptosisToken	A-Cry- Crypt/01- 08-18/24
Ctest7 Project					
Ctest7					
	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.co m/BlockChainsSec urity/EtherTokens /tree/master/CTe st7, https://github.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 Ointeger%20overf low.md	A-Cte- Ctest/01- 08-18/25
Cws Project					
CWS	00.05.0010		mlm.l .c	1 //	1.0
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.co m/BlockChainsSec urity/EtherTokens /tree/master/CW S, https://github.co m/BlockChainsSec	A-Cws- CWS/01- 08-18/26
CV Scoring Scale (CVSS	s)	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
				urity/EtherTokens /blob/master/GE MCHAIN/mint%2 0integer%20overf low.md	
Databits Project	ct				
Databits		_		1	
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 Ointeger%20overf low.md	A-Dat- Datab/01 -08- 18/27
Destineed Proj	ect				
Destineed					
Overflow Deweisecurity:	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
Deweisecuritys		Tojett			
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 Ointeger%20overf	A-Dew- Dewei/01 -08- 18/29
CV Scoring Scale (CV	VSS)	3-4	4-5 5-6 6-7	7-8 8-9	9-10
	(s): CSRF-Cross Site		orgery; Dir. TravDirectory Traversal; D	oS-Denial of Service; NA- No	ot Applicable;

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	'	
Dinsteincoin P	roject				
Overflow 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	m/BlockChainsSec urity/EtherTokens /tree/master/Din steinCoin,	A-Din- Dinst/01- 08-18/30
Dopnetwork P	roject				
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	m/BlockChainsSec urity/EtherTokens /tree/master/dop network,	A-Dop- Dopne/01 -08- 18/31
Eastcoin Proje	ct				
Overflow	09-07-2018	5	The mintToken function of a smart contract implementation for Eastcoin, an Ethereum	m/BlockChainsSec	A-Eas- Eastc/01- 08-18/32

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/GE MCHAIN/mint%2 0integer%20overf low.md,	
				https://github.co m/BlockChainsSec urity/EtherTokens /tree/master/East coin	
Easticoin Proje	ect				
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.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 0integer%20overf low.md,	A-Eas- Easti/01- 08-18/33
				https://github.co m/BlockChainsSec urity/EtherTokens /tree/master/East icoin	
Eddtoken Proj	ect				
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	1 //0	A-Edd- Eddto/01 -08- 18/34
Elearningcoine	erc Project				
Elearningcoine					
Overflow	09-07-2018	5	The mintToken function of a	https://github.co	A-Ele-
CV Scoring Scale (CV		3-4	4-5 5-6 6-7 orgery; Dir. TravDirectory Traversal; Do	7-8 8-9	9-10

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/BlockChainsSec urity/EtherTokens /tree/master/ELe arningCoinERC, https://github.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 Ointeger%20overf low.md	Elear/01- 08-18/35
Entercoin Proj	ect				
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.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 Ointeger%20overf low.md, https://github.co m/BlockChainsSec urity/EtherTokens /tree/master/Ent erCoin	A-Ent- Enter/01- 08-18/36
Entertoken Pro	oject				
Eristicaico Pro	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.co m/BlockChainsSec urity/EtherTokens /tree/master/Ent erToken, https://github.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 Ointeger%20overf low.md	A-Ent- Enter/01- 08-18/37
Li isticalco i'10	ject				

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

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 EristicalCO, 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.co m/BlockChainsSec urity/EtherTokens /tree/master/Eris ticaICO, https://github.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 Ointeger%20overf low.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.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 Ointeger%20overf low.md, https://github.co m/BlockChainsSec urity/EtherTokens /tree/master/ESH	A-Esh- ESH/01- 08-18/39
Essence Projec	:t				
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.co m/BlockChainsSec urity/EtherTokens /tree/master/Ess ence, https://github.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 Ointeger%20overf low.md	A-Ess- Essen/01- 08-18/40
CV Scoring Scale (C	-	3-4	4-5 5-6 6-7 orgery; Dir. TravDirectory Traversal; Do	7-8 8-9	9-10

018 5	s f H c c	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 get the	https://github.co m/BlockChainsSec urity/EtherTokens /blob/master/GE	A-Exa- Exaco/01-
018 5	s f H c c	smart contract implementation for ExacoreContract, an Ethereum token, has an integer overflow that allows the owner	m/BlockChainsSec urity/EtherTokens /blob/master/GE	Exaco/01-
5	s f H c c	smart contract implementation for ExacoreContract, an Ethereum token, has an integer overflow that allows the owner	m/BlockChainsSec urity/EtherTokens /blob/master/GE	Exaco/01-
		of the contract to set the balance of an arbitrary user to any value. CVE-ID:CVE-2018-13771	MCHAIN/mint%2 Ointeger%20overf low.md, https://github.co m/BlockChainsSec urity/EtherTokens /tree/master/Exa coreContract	08-18/41
018 5	s f t t	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.co m/BlockChainsSec urity/EtherTokens /tree/master/exs ulcoin, https://github.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 Ointeger%20overf low.md	A-Exs- Exsul/01- 08-18/42
018 4.3	i a f f l t c c c l	dereference while converting a crafted AVI file to MPEG4, eading to a denial of service.	https://github.co m/FFmpeg/FFmp eg/commit/00e81 81bd97c834fe607 51b0c511d4bb97 875f78	A-Ffm- Ffmpe/01 -08- 18/43
	3-4	4-5 5-6 6-7	7-8 8-9	9-10
	3	3-4	trigger a NULL pointer dereference while converting a crafted AVI file to MPEG4, leading to a denial of service. CVE-ID:CVE-2018-13303	trigger a NULL pointer dereference while converting a crafted AVI file to MPEG4, leading to a denial of service. CVE-ID:CVE-2018-13303

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_head er 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.co m/FFmpeg/FFmp eg/commit/2aa90 47486dbff12d9e0 40f917e5f799ed2f d78b	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.co m/FFmpeg/FFmp eg/commit/bd27a 9364ca274ca97f1 df6d984e88a0700 fb235	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	m/FFmpeg/FFmp eg/commit/95556	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.co m/FFmpeg/FFmp eg/commit/d08d4 a8c7387e758d439 b0592782e4cfa2b 4d6a4	A-Ffm- Ffmpe/01 -08- 18/47

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

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_INDEPEN DENT) 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.debi an.org/security/2 018/dsa-4249, https://github.co m/FFmpeg/FFmp eg/commit/ed22d c22216f74c75ee7 901f82649e1ff725 ba50	A-Ffm- Ffmpe/01 -08- 18/48
Finaltoken Pro	oject				
Overflow	09-07-2018	5	The mintToken function of a	https://github.co	A-Fin-
Futurxe Projec		3	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	m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 0integer%20overf low.md, https://github.co m/BlockChainsSec urity/EtherTokens /tree/master/Fina lToken	Final/01- 08-18/49
Futurxe Futurxe	, t				
Overflow	09-07-2018	5	The mintToken function of a	https://github.co	A-Fut-
Overnow	07 07 2010		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	m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 0integer%20overf low.md,	Futur/01- 08-18/50
CV Scoring Scale (C	VSS)	3-4	4-5 5-6 6-7	7-8 8-9	9-10
		Request F	orgery; Dir. TravDirectory Traversal; Do	oS-Denial of Service; NA- N	ot Applicable;

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Reference/Patch	NCIIPC ID
				https://github.co m/BlockChainsSec urity/EtherTokens /tree/master/Fut urXe	
Gfcb Project					
Gfcb	20.07.2010	_			
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.co m/BlockChainsSec urity/EtherTokens /tree/master/GFC B, https://github.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 Ointeger%20overf low.md	A-Gfc- Gfcb/01- 08-18/51
Globalsuperga	metoken Proje	ct			
Globalsuperga	metoken				
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.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 0integer%20overf low.md, https://github.co m/BlockChainsSec urity/EtherTokens /tree/master/Glo balSuperGameTok en	A-Glo- Globa/01- 08-18/52
Globecoin Proj	ect				
Globecoin	12.07.2010	2	An integer ever	https://github.cs	A Cla
Overflow	12-07-2018	5	An integer overflow vulnerability exists in the function transfer_tokens_after_ICO of GlobeCoin (GLB), an Ethereum	https://github.co m/VenusADLab/E therTokens/tree/ master/GlobeCoin %28GLB%29,	A-Glo- Globe/01- 08-18/53
CV Scoring Scale (C	VSS)	3-4	4-5 5-6 6-7	7-8 8-9	9-10
		Request F	orgery; Dir. TravDirectory Traversal; Do	oS-Denial of Service; NA- No	ot Applicable;

Token smart contract An attacker could use it to set any user's balance. CVE-ID:CVE-2018-14004 CVE-ID:CVE-2018-13694 C	Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Reference/Patch	NCIIPC ID
Overflow Overfl				attacker could use it to set any user's balance.	m/VenusADLab/E therTokens/blob/ master/SHARKTE CH/SHARKTECH.	
Overflow 09-07-2018 5						
Overflow Overfl		09-07-2018	5	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.	m/BlockChainsSec urity/EtherTokens /tree/master/GMi le, https://github.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 Ointeger%20overf	Gmile/01-
Overflow O9-07-2018 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 The mintToken function of a smart contract implementation m/BlockChainsSec urity/EtherTokens /tree/master/Gol dTokenERC20, https://github.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 Ointeger%20overf low.md						
dominieworia i roject	Overflow	09-07-2018	5	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.	m/BlockChainsSec urity/EtherTokens /tree/master/Gol dTokenERC20, https://github.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 Ointeger%20overf	Goldt/01-
Gomineworld		Project				

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

7-2018 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.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 Ointeger%20overf low.md, https://github.co m/BlockChainsSec urity/EtherTokens /tree/master/Go MineWorld	A-Gom- Gomin/01 -08- 18/56
7-2018 5			IVITITE VV OT IU	
7-2018 5				
7-2018 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.co m/BlockChainsSec urity/EtherTokens /tree/master/Goo chain, https://github.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 Ointeger%20overf low.md	A-Goo- Gooch/01 -08- 18/57
oject		,		
7-2018 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.co m/BlockChainsSec urity/EtherTokens /tree/master/Gre enEnergyToken, https://github.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 Ointeger%20overf low.md	A-Gre- Green/01 -08- 18/58
	3-4	4-5 5-6 6-7	7-8 8-9	9-10
			3-4 4-5 5-6 6-7 Cross Site Request Forgery; Dir. TravDirectory Traversal; Do	/blob/master/GE MCHAIN/mint%2 0integer%20overf low.md

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.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 0integer%20overf low.md, https://github.co m/BlockChainsSec urity/EtherTokens /tree/master/HEY	A-Hey- HEY/01- 08-18/59
Hormitechtok	en Project				
Hormitechtoke	n				
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.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 0integer%20overf low.md, https://github.co m/BlockChainsSec urity/EtherTokens /tree/master/Hor mitechToken	A-Hor- Hormi/01 -08- 18/60
Hyipcrowdsale	e1 Project				
Hyipcrowdsale	1				
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.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 0integer%20overf low.md, https://github.co m/BlockChainsSec urity/EtherTokens /tree/master/HYI PCrowdsale1	A-Hyi- Hyipc/01- 08-18/61
CV Scoring Scale (C	VSS)	3-4	4-5 5-6 6-7	7-8 8-9	9-10
	(s): CSRF-Cross Site		orgery; Dir. TravDirectory Traversal; D	oS-Denial of Service; NA- No	ot Applicable;

 ${\bf Sql\text{-}SQL\ Injection;\ XSS\text{-}\ Cross\ Site\ Scripting;}$

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Reference/Patch	NCIIPC ID
Hyiptoken Pro	ject				
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.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 0integer%20overf low.md, https://github.co m/BlockChainsSec urity/EtherTokens /tree/master/HYI PToken	A-Hyi- Hyipt/01- 08-18/62
Ico Dollar Proj	ect				
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.co m/BlockChainsSec urity/EtherTokens /tree/master/ICO Dollar, https://github.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 0integer%20overf low.md	A-Ico- Ico/01- 08-18/63
Ideacoin Proje	ct				
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 The mintToken function of a m/BlockChainsSec urity/EtherTokens /tree/master/Idea Coin,https://github.com/BlockChain sSecurity/EtherTokens /tree/master/Idea Coin,https://github.com/BlockChainsSec urity/EtherTokens /tree/master/Idea /tree/master		A-Ide- Ideac/01- 08-18/64
	/SS)	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
Instacocoa Pro	ject				
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	art contract implementation Instacocoa, an Ethereum ten, has an integer overflow at allows the owner of the attract to set the balance of arbitrary user to any value. m/BlockChainsSec urity/EtherTokens /tree/master/Inst acocoa, https://github.co	
Ipmcoin Projec	ct				
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	m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2	A-Ipm- Ipmco/01 -08- 18/66
Iseevoicetoker	n 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	contract implementation ISeeVoiceToken, an eum token, has an integer ow that allows the owner econtract to set the ce of an arbitrary user to llue. m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 0integer%20overf low.md,	
CV Scoring Scale (C	VSS)	3-4	4-5 5-6 6-7	7-8 8-9	9-10
		Request F	orgery; Dir. TravDirectory Traversal; D	oS-Denial of Service; NA- N	ot Applicable;

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Reference/Patch	NCIIPC ID
				/tree/master/ISee VoiceToken	
Jeanstoken Pro	oject				
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.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 0integer%20overf low.md, https://github.co m/BlockChainsSec urity/EtherTokens /tree/master/Jean	A-Jea- Jeans/01- 08-18/68
Livesiteles Du	oio at			sToken	
Jiucaitoken Pro	oject				
Overflow	09-07-2018	5	The mintToken function of a	httma.//aithub.ao	A-Jiu-
Overnow	09-07-2010	3	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.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 0integer%20overf low.md, https://github.co m/BlockChainsSec urity/EtherTokens /tree/master/Jiuc aiToken	Jiuca/01- 08-18/69
Jixocoin Projec	et				
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.co		A-Jix- Jixoc/01- 08-18/70
CV Cooring C1- (C)	VCC)	3-4	4-5 5-6 6-7	7-8 8-9	9-10
CV Scoring Scale (CV					
Vulnerability Type(orgery; Dir. TravDirectory Traversal; Do	oS-Denial of Service; NA- No	ot Applicable;

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Reference/Patch	NCIIPC ID
				m/BlockChainsSec urity/EtherTokens /tree/master/Jixo Coin	
Jpmd100b Pro	ject				
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.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 Ointeger%20overf low.md, https://github.co m/BlockChainsSec urity/EtherTokens	A-Jpm- Jpmd1/01 -08- 18/71
				/tree/master/JPM D100B	
Justwallet Proj	ject				
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.co m/BlockChainsSe		A-Jus- Justw/01- 08-18/72
				urity/EtherTokens /tree/master/Just	
Kbit Project				Wallet	
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.co m/BlockChainsSec urity/EtherTokens /tree/master/kBit , https://github.co m/BlockChainsSec	A-Kbi- Kbit/01- 08-18/73
CV Scoring Scale (C	VSS)	3-4	4-5 5-6 6-7	7-8 8-9	9-10
Vulnerability Type		_	orgery; Dir. TravDirectory Traversal; Do	oS-Denial of Service; NA- No	ot Applicable;

Vulnerability Type(s)	Publish Date	cvss	Descrip	tion & CVE	: ID	Reference/	Patch	NCIIPC ID
			CVE-ID:CVE	-2018-137	46	urity/EtherT/blob/maste MCHAIN/mi Ointeger%20 low.md	er/GE nt%2	
Kissme Project	t							
Kissme								
Overflow	09-07-2018	5	The mintTo smart contrator KissMe, a has an interact to an arbitrary CVE-ID:CVE	nn Ethereunger overfloo owner set the bal	entation n token, ow that of the ance of y value.	https://githum/BlockChaurity/EtherT/tree/masteMe, https://githum/BlockChaurity/EtherT/blob/masteMCHAIN/miOinteger%20low.md	insSec Cokens r/Kiss ab.co insSec Cokens er/GE nt%2	A-Kis- Kissm/01 -08- 18/74
Landcoin Proje	ect							
Landcoin Overflow	09-07-2018	5	The mintTo smart contract to token, has a that allows contract to an arbitrary CVE-ID:CVE	n, an Et n integer o the owner set the bal user to an	entation hereum verflow of the ance of y value.	https://githum/BlockChaurity/EtherT/blob/masteMCHAIN/miOinteger%20low.md, https://githum/BlockChaurity/EtherT/tree/masteoken	insSec Cokens er/GE nt%2 Doverf ub.co insSec Cokens	A-Lan- Landc/01 -08- 18/75
Overflow	09-07-2018	5	The mintTo smart contrator LandCo token, has a that allows contract to an arbitrary CVE-ID:CVE	act implements in, an Et in integer of the owner set the balance is an integer to an i	entation hereum verflow of the ance of y value.	https://githum/BlockChaurity/EtherT/blob/masteMCHAIN/miOinteger%20low.md,	insSec Cokens er/GE nt%2 Doverf	A-Lan- Landc/01 -08- 18/76
CV Scoring Scale (C	VSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10
	(s): CSRF-Cross Site	Request F	orgery; Dir. Trav	Directory Tr	aversal; Do	S-Denial of Servi	ce; NA- No	ot Applicable;

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Reference/Patch	NCIIPC ID
			m/BlockChainsSe urity/EtherToken /tree/master/Lar dCoin		
Lexittoken Pro	ject				
Lexittoken		T .			
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.co m/BlockChainsSec urity/EtherTokens /tree/master/Lexi tToken, https://github.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 0integer%20overf low.md	A-Lex- Lexit/01- 08-18/77
Lolicoin Projec	t				
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.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 0integer%20overf low.md, https://github.co m/BlockChainsSec urity/EtherTokens /tree/master/Loli Coin	A-Lol- Lolic/01- 08-18/78
Lottery Project	t				
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.co		A-Lot- Lotte/01- 08-18/79
CV Scoring Scale (CV	VSS)	3-4	4-5 5-6 6-7	7-8 8-9	9-10
	(s): CSRF-Cross Site		orgery; Dir. TravDirectory Traversal; Do	oS-Denial of Service; NA- No	ot Applicable;

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Reference/Patch	NCIIPC ID
			CVE-ID:CVE-2018-13678	m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 0integer%20overf low.md	
Malaysia Coins					
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.co m/VenusADLab/E therTokens/tree/ master/Malaysia %20coins%28Xmc %29, https://github.co m/VenusADLab/E	A-Mal- Malay/01 -08- 18/80
Malltoken Proj	ect			therTokens/blob/ master/SHARKTE CH/SHARKTECH. md	
Malltoken				1	
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.co m/BlockChainsSec urity/EtherTokens /tree/master/Mall Token, https://github.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 Ointeger%20overf low.md	A-Mal- Mallt/01- 08-18/81
Mehditazitoken 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.co m/BlockChainsSec urity/EtherTokens /tree/master/Meh diTAZIToken,	A-Meh- Mehdi/01 -08- 18/82
				·	

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.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 0integer%20overf low.md	
Mjolnir Projec	t				
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.co m/BlockChainsSec urity/EtherTokens /tree/master/Mjol nir, https://github.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 Ointeger%20overf low.md	A-Mjo- Mjoln/01- 08-18/83
Moneychainne	t Project				
Moneychainne					
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.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 Ointeger%20overf low.md, https://github.co m/BlockChainsSec urity/EtherTokens /tree/master/Mon eyChainNetToken	A-Mon- Money/0 1-08- 18/84
Mp3 Coin Proje	ect				
Mp3 Coin Overflow	12-07-2018	5	An integer overflow vulnerability exists in the function distribute of MP3	https://github.co m/VenusADLab/E therTokens/tree/	A-Mp3- Mp3/01- 08-18/85
CV Scoring Scale (C	VSS)	3-4	4-5 5-6 6-7	7-8 8-9	9-10
Vulnerability Type	(s): CSRF-Cross Site	Request F	orgery; Dir. TravDirectory Traversal; Do	S-Denial of Service; NA- No	ot Applicable;

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%20C oin%28MP3%29, https://github.co m/VenusADLab/E therTokens/blob/ master/SHARKTE CH/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.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 0integer%20overf low.md, https://github.co m/BlockChainsSec urity/EtherTokens /tree/master/MyY LCToken	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.co m/BlockChainsSec urity/EtherTokens /tree/master/NCU , https://github.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 Ointeger%20overf low.md	A-Ncu- NCU/01- 08-18/87
Neo Genesis To					
Neo Genesis To	ken				

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
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	A-Neo- Neo/01- 08-18/88	
Netkilleradvar			ect		
Netkilleradvan	1				
Overflow	09-07-2018	5	The mintToken function of a smart contract implementation for NetkillerAdvancedTokenAirDr op, 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.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 Ointeger%20overf low.md, https://github.co m/BlockChainsSec urity/EtherTokens /tree/master/Net killerAdvancedTo kenAirDrop	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.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 Ointeger%20overf low.md, https://github.co m/BlockChainsSec urity/EtherTokens /tree/master/Net killerToken	A-Net- Netki/01- 08-18/90
CV Scoring Scale (C	VSS)	3-4	4-5 5-6 6-7	7-8 8-9 S-Denial of Service; NA- No	9-10

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	mart contract implementation r normikaivo, an Ethereum ken, has an integer overflow at allows the owner of the ntract to set the balance of arbitrary user to any value. m/BlockChainsSec urity/EtherTokens /tree/master/nor mikaivo, https://github.co						
Obtcoin Projec	:t									
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.co m/BlockChainsSec urity/EtherTokens /tree/master/OBT Coin, https://github.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 Ointeger%20overf low.md	A-Obt- Obtco/01- 08-18/92					
Onechain Proje	ect									
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 The mintToken function of a m/BlockChains witty/EtherTok (Chain, https://github.m/BlockChains urity/EtherTok /blob/master/6/blob/master/6/blob/master/6/blob/mintfo		A-One- Onech/01 -08- 18/93					
CV Coording C. 1. (C)	uce)	3-4	4-5 5-6 6-7	7-8 8-9	9-10					
CV Scoring Scale (CV			orgery; Dir. TravDirectory Traversal; Do							

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Reference/Patch	NCIIPC ID
				0integer%20overf low.md	
Oracle					
Agile Product L	ifecycle Manag	ement F	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		A-Ora- Agile/01- 08-18/94
Applications M				NA	T
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	A-Ora- Appli/01- 08-18/95	
CV Scoring Scale (C	VSS)	3-4	4-5 5-6 6-7	7-8 8-9	9-10
Vulnerability Type(_	orgery; Dir. TravDirectory Traversal; I	oS-Denial of Service; NA- N	ot Applicable;

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID			Reference	/Patch	NCIIPC ID
			Applications Successful vulnerability unauthorized data or come Oracle Applications Oracle Applications Score 7.5 impacts). (CVSS:3.0/All :N/S:U/C:H/CVE-ID:CVE	attacks of y can rest access to applete accessolications Mata. CVSS 3 (Confider CVSS). V:N/AC:L/F/I:N/A:N).	critical strong to all Manager s.0 Base entiality Vector: PR:N/UI			
Banking Corpo								
DoS	18-07-2018	5.5	Banking Component Services (subcomponent Supported affected and 12.5.0, 14.0. exploitable allows low with network to comprom Corporate I attacks of the result in uninsert or deformation of Oracle I Lending acunauthorized partial deformation of the component of	of Oracle Final Applipment: Core in versions the 12.3.0, 0 and 14.1.0 vulne privileged ark access vinise Oracle Interest of the ending. Surisis vulnerable authorized lete access to cessible day ability to enial of ending of orporate Laber Base Scoand Ava CVSS V:N/AC:L/F/I:L/A:L).	Lending inancial ications nodule). nat are 12.4.0, in Easily erability attacker a HTTP Banking ccessful ility can update, to some rporate and cause a service Oracle lending. re 5.4 ilability Vector: PR:L/UI	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

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
			Services (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-0ra- 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)	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 (CV Vulnerability Type)		3-4 Request F	4-5 5-6 6-7 orgery; Dir. TravDirectory Traversal; Do	7-8 8-9 S-Denial of Service; NA- N	9-10 ot Applicable;

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-0ra- 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)	blish 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		
	3-07-2018	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		A-Ora- Banki/01- 08- 18/102
			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		Banki/01- 08- 18/103
CV Scoring Scale (CVSS)		3-4	4-5 5-6 6-7 orgery; Dir. TravDirectory Traversal; I	7-8 8-	

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

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

Vulnerability Type(s)	Publish Date	cvss	Descrip	otion & CVE	ID	Reference/	'Patch	NCIIPC ID
			accessible unauthorize subset of Corporate data. CVSS (Confidential impacts). (CVSS:3.0/A:R/S:C/C:L/CVE-ID:CVE	ed read acce Oracle I Lending acc 3.0 Base Sc ality and In CVSS V:N/AC:L/F I:L/A:N).	ess to a Banking cessible ore 6.1 ntegrity Vector: PR:N/UI			
Banking Paym								
DoS	18-07-2018	5.5	Banking Payof Oracle Applications Payments versions that 12.2.0, 12.3 and 14.1.0. vulnerability privileged network accompromise Payments. of this vulnin unauthor or delete a Oracle Baccessible unauthorize partial de	Financial S s (subcom Core). Sup at are affect 3.0, 12.4.0, Easily exp y allows attacker cess via H e Oracle I Successful erability care cess to s anking Pa data ed ability to enial of OOS) of syments. CV 5.4 (Integr impacts). AV:N/AC:L/F /I:L/A:L).	ponent services ponent: oported ted are 12.5.0 loitable low with TTP to Banking attacks a result ome of yments and cause a service Oracle VSS 3.0 ity and CVSS	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					A-Ora- Banki/01- 08- 18/106
CV Scoring Scale (C	VCC)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

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
			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)	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-0ra- Banki/01- 08- 18/109

- 1						- 0	0.0	
	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
			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

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
NA 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-0ra- Banki/01- 08- 18/112

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
			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-0ra- 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)	Publish Date	cvss	Descri	ption & CVE	EID	Reference/	Patch	NCIIPC ID
- 9 P C ()			CVE-ID:CVI	E-2018-289	6			
Business Intelli	igence Publishe	er						
NA	18-07-2018	4	Supported affected 11.1.1.9.0, 12.2.1.3.0. vulnerabilit privileged network accompromise Successful vulnerabilit unauthorized data or com BI Published CVSS 3.0 (Confidential Vector: (CVSS:3.0/A:N/S:U/C:H, CVE-ID:CVE	mponent of Middenent: Web Services to Avenue attacks of access to all the access to all the access of all the Middenent of the access of access to all the access of acces	dleware Server). hat are .1.1.7.0, and loitable low with TTP to blisher. of this sult in critical as to all he data. re 6.5 s). CVSS	NA		A-Ora- Busin/01- 08- 18/114
NA	18-07-2018	6.4	•	omponent of Midonent: BI Pusted are 11 12.2.1.2.0 Easily expected attack excess via Health attacks of Commodification data or excessible of Midone Mi	dleware ablisher versions and loitable allows er with TTP to ablisher. of this sult in reation, a access all BI data as	NA		A-Ora- Busin/01- 08- 18/115
CV Scoring Scale (C	VSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	cvss	Desc	ription & CVE	: ID	Reference/	Patch	NCIIPC ID
			Publisher 3.0 B (Confident impacts). (CVSS:3.0 :N/S:U/C:	a subset accessible datase Score tiality and In CVSS /AV:N/AC:L/F L/I:H/A:N). VE-2018-295	ta. CVSS 8.2 ntegrity Vector: PR:N/UI			
NA	18-07-2018	6.4	Vulneral Publisher Fusion (subcomp The supp affected exploitability allows attacker via HTTI Publisher this vulne unauthor deletion of to critic Publisher well as access the Publisher 3.0 B (Confident impacts). (CVSS:3.0 :N/S:U/C:	oility in to component or Mide onent: Layout orted version is 11.1.7.0. It will network or to comprore a Successful at the example of a subset accessible data are accessible data ase Score tiality and Interest of the example of the	he BI f Oracle dleware trools). that is Easily erability nticated access nise BI tacks of esult in reation, naccess all BI data as d read of BI ta. CVSS 8.2 ntegrity Vector: PR:N/UI	NA		A-Ora- Busin/01- 08- 18/116
Business Process		t Suite						
NA	18-07-2018	6.4	Business Suite co Fusion (subcomp Analysis Supported affected 11.1.1.9.0	onent: & Diso d versions tl	gement Oracle dleware Process covery). hat are .1.1.7.0,	NA		A-Ora- Busin/01- 08- 18/117
CV Scoring Scale (CVS	SS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	cvss	Descrip	otion & CVE	ID 1	Reference/	Patch	NCIIPC ID
			Management attacks of the result in creation, modification data or all Process Maccessible unauthorized data or conforacle Banagement data. CVSS (Confidential	unauther th network to compusiness at Suite. Suite sis vulnerabit a unaut deletion access to l Oracle B lanagement data as ver data as ver ed access to aplete acces usiness at Suite acces at Suite acces at Suite acces ality and In CVSS av:N/AC:L/F /I:H/A:N).	access promise Process ccessful dity can horized or critical cusiness Suite well as critical es to all Process cessible fore 9.1 integrity Vector: PR:N/UI			
Communication	ns Convergence		CVL ID.CVL	2010 310				
NA	18-07-2018	5.8	Communica Server com Communica (subcompor The suppor affected exploitable allows attacker wi via HTTP Oracle Messaging	nponent of tions Appliant: Web ted version is 3.x. vulne unauther th network to compunities of the attack vulnerability Communities of the attack vulnerability commun	oracle ications Client). that is Easily erability nticated access oromise ications ccessful human person ter and y is in ications cks may	NA		A-Ora- Commu/0 1-08- 18/118
CV Scoring Scale (C	VSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

CV Scoring Scale (CVSS)

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

Vulnerability Type(s)	Publish Date	cvss	Descrip	otion & CVE	ID	Reference/	Patch	NCIIPC ID
			products. So this vulnera unauthorized delete access Communicated Server access as unauthorized as unauthorized Server access and Basic (Confidential impacts). (CVSS:3.0/A:R/S:C/C:L/CVE-ID:CVE	ability can red update, in set o some or tions Me ssible data rized read act of tions Me essible data e Score ality and In CVSS V:N/AC:L/F I:L/A:N). 1-2018-293	esult in asert or f Oracle ssaging as well ccess to Oracle ssaging a. CVSS 6.1 attegrity Vector: PR:N/UI			
Communication							Ţ	
NA	18-07-2018	6.4	Communica Application component Communica (subcompor supported affected exploitable allows attacker wi via HTTP Oracle Com	of tions Applianent: GUI) version to the second attacks of the second accellate. Proceed accellate. Procedure attacks of the second accellate. CVSS 3	ocessor Oracle ications The hat is Easily brability inticated access bromise EAGLE bocessor of this sult in insert or f Oracle iE LNP ocessor vell as ess to a Oracle iE LNP ocessor . Of asse	NA		A-Ora- Commu/0 1-08- 18/119
CV Scoring Scale (CV	(SS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

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

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 Rela	tionship Manag	ement '	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
		3-4	4-5 5-6 6-7	7-8 8-9	9-10

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	NCIIPC ID	
NA 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 Serv	er				
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-0ra- Datab/01 -08- 18/122
CV Scoring Scale (C	VSS)	3-4	4-5 5-6 6-7	7-8 8-9	9-10
Vulnerability Type	(s): CSRF-Cross Site	Request F	orgery; Dir. TravDirectory Traversal; Do	oS-Denial of Service; NA- N	ot 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)	Publish Date	cvss	Description & CV	E ID	Reference/Pa	atch NCIIPC ID
			impacts). CVSS (CVSS:3.0/AV:L/AC:L, N/S:C/C:N/I:H/A:H). CVE-ID:CVE-2018-29	•		
E-business Suit	te					
NA	18-07-2018	5	Vulnerability in the Application Object component of Or Business (subcomponent: Atta / File Upload). The second that is affile 12.1.3. Easily expended that is affile 12.1.3.	Library acle E- Suite schments upported ected is aploitable allows eker with HTTP to Oracle Library. of this esult in insert or of Oracle Library 3.0 Base impacts). Vector: /PR:N/UI	NA	A-Ora-E- bus/01- 08- 18/124
_	nager Ops Cent					
NA	18-07-2018	6.4	Networking). The s version that is aff 12.2.2. Easily ex vulnerability unauthenticated attac network access via compromise E Manager Ops Successful attacks	er Ops of Oracle Products inponent: upported ected is eploitable allows eker with HTTP to interprise Center. of this	NA	A-Ora- Enter/01- 08- 18/125
CV Scoring Scale (C	VSS)	3-4	4-5 5-6	6-7	7-8	8-9 9-10
		Request F	orgery; Dir. TravDirectory	Traversal; Do	S-Denial of Service	; NA- Not Applicable;

Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	cvss	Descrip	otion & CVE	ID	Reference/	Patch	NCIIPC ID
			vulnerability unauthorize data or com Enterprise Center acce as unauthor or delete a Enterprise Center acce 3.0 Base (Confidential impacts). (CVSS:3.0/A :N/S:U/C:H/ CVE-ID:CVE	d access to applete access Manager ssible data access to so Manager essible data e Score ality and In CVSS V:N/AC:L/P/I:L/A:N).	critical s to all Ops as well e, insert ome of Ops a. CVSS 8.2 ntegrity Vector:			
Flexcube Enter	prise Limits An	d Collat	eral Manage	ment	<u> </u>			
DoS	18-07-2018	5.5	FLEXCUBE and Collat component Services (subcompor Infrastructu versions that 12.3.0, 14.0. exploitable allows low with networ to compound FLEXCUBE and Collate Successful vulnerability unauthorized delete access FLEXCUBE and Collate accessible unauthorized partial delete accessible unauthori	eral Mana of Oracle Fi Appli nent: re). Sup at are affec 0 and 14.1.0 vulne privileged a rk access via bromise Enterprise eral Manag attacks o y can res d update, ir s to some of Enterprise eral Mana data d ability to nial of OOS) of Enterprise	Limits gement nancial acations oported ted are 0. Easily rability attacker a HTTP Oracle Limits gement. of this sult in asert or f Oracle Limits gement and cause a service Oracle Limits gement.	NA		A-Ora- Flexc/01- 08- 18/126
CV Scoring Scale (C	VSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

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
			(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)	Publish Date	cvss	Description & CVE ID	Reference/Patch	NCIIPC ID
NA 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-0ra- 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)	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

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

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

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
			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-0ra- Flexc/01- 08- 18/133
CV Scoring Scale (CV		3-4	4-5 5-6 6-7 lorgery; Dir. TravDirectory Traversal; Do	7-8 8-9	9-10

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)	Publish Date	cvss	Descrip	otion & CVE	Reference/	Patch	NCIIPC ID	
			delete access FLEXCUBE and Collate accessible unauthorize subset of Enterprise Collateral accessible of Score 6.1 (Gintegrity Vector: (CVSS:3.0/A:R/S:C/C:L/CVE-ID:CVE	Enterprise eral Mana data as ved read acceloracie FLI Limits Mana data. CVSS 3 Confidential impacts). V:N/AC:L/FI:L/A:N).	Limits gement vell as ess to a EXCUBE and gement .0 Base ity and CVSS			
Flexcube Inves	tor Servicing				-			
DoS	18-07-2018	5.5	FLEXCUBE component Services (subcompor Infrastructu versions the 12.0.4, 12 12.4.0. Evulnerability privileged network accompromise Investor Seattacks of the result in uninsert or de of Oracle F Servicing acunauthorize partial de	of Oracle Finapple Applement: re). Supart are affect and Avact Applement are affect are affect attacker attacker attacker attacker attacker attacker attacker attacker attacker authorized authorized attacker access to a Applement a Ap	ervicing inancial ications oported ted are 0 and loitable low with TTP to EXCUBE ccessful dity can update, to some investor ata and cause a service Oracle rvicing. re 5.4 ilability Vector:	NA		A-Ora- Flexc/01- 08- 18/135
CV Scoring Scale (C)		3-4	4-5	5-6	6-7	7-8	8-9	9-10

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
			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
-------------------------	-----	-----	-----	-----	-----	-----	------

FLEXCUBE Investor Servicing component of Oracle Financial 08-	Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Reference/Patch	NCIIPC ID
(CVSS·3.0/AV·N/AC·L/PR·L/III		18-07-2018	4	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 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		A-Ora- Flexc/01- 08- 18/138
:N/S:U/C:N/I:N/A:H). CVE-ID:CVE-2018-3030	NA	18-07-2018	4.9	:N/S:U/C:N/I:N/A:H). CVE-ID:CVE-2018-3030 Vulnerability in the Oracle FLEXCUBE Investor Servicing	NA	A-Ora- Flexc/01-

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
			Services (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)	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

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
NA 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

CV Scoring Scale (CVSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10
ev scoring scale (evss)							

Vulnerability Type(s)	Publish Date	cvss	Descripti	on & CVE	: ID	Reference/	Patch	NCIIPC ID
			Servicing, significantly in products. Such this vulnerable unauthorized delete access to FLEXCUBE In accessible data unauthorized subset of On Investor Service data. CVSS 3.0 (Confidentiality)	he attack lnerability CUBE I attacks in attacks in the control of the control of the cube in the cube	ter and y is in nvestor may ditional tacks of esult in a sert or f Oracle ervicing vell as ess to a EXCUBE cessible fore 6.1 antegrity Vector: PR:N/UI			
Flexcube Unive	rsal Banking							
DoS	18-07-2018	5.5	Vulnerability FLEXCUBE Un component of Services (subcomponent Infrastructure versions that 11.3.0, 11.4.0 12.0.3, 12.1.0 12.4.0, 14.0.0 exploitable allows low pr with network to compre FLEXCUBE Un Successful a vulnerability unauthorized delete access of FLEXCUBE Un accessible unauthorized	niversal I Oracle Fi Appliant:). Supare affect), 12.0.1,), 12.2.0, and 14.1.0 vulne rivileged a access vi omise niversal B ttacks of can res update, in to some o niversal I data	Banking inancial ications operted ted are 12.0.2, 12.3.0, 0. Easily erability attacker a HTTP Oracle banking. of this sult in insert or f Oracle Banking and	NA		A-Ora- Flexc/01- 08- 18/144
CV Scoring Scale (C	1100)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

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
			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)	Publish Date	cvss	Description & CVE ID	Reference/Patch	NCIIPC ID
NA 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
j , ,							

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
9 ()							

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	

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
			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

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
			(CVSS:3.0/AV:N/AC:L/PR:L/U: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 Financia Services Application (subcomponent: Infrastructure). Supported versions that are affected and 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 accessiva HTTP to compromise Oracle FLEXCUBE Universal Banking. Successful attack 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 thi vulnerability can result in unauthorized update, insert of delete access to some of Oracle FLEXCUBE Universal Banking accessible data as well a unauthorized read access to subset of Oracle FLEXCUBE Universal Banking accessible data. CVSS 3.0 Base Score 6.6 (Confidentiality and Integrity impacts). CVSS Vector (CVSS:3.0/AV:N/AC:L/PR:N/U:R/S:C/C:L/I:L/A:N). CVE-ID:CVE-2018-2899		A-Ora-Flexc/01-08-18/152
Fusion Middlev	vare Mapviewe	r	C. E IDIGIE HOLD HOTT		
NA	18-07-2018	7.5	Vulnerability in the Oracle Fusion Middleware		A-Ora- Fusio/01-
CV Scoring Scale (C	VSS)	3-4	4-5 5-6 6-7	7-8 8-9	9-10
Vulnerability Type	(s): CSRF-Cross Site	Request F	orgery; Dir. TravDirectory Traversal;	DoS-Denial of Service; NA- N	ot Applicable;

Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	cvss	Descrip	otion & CVE	ID	Reference/	Patch	NCIIPC ID
			MapViewer Oracle Fu (subcompor Supported affected ar 12.2.1.3.0. vulnerability unauthentic network ac compromise Middleware Successful vulnerability takeover of Middleware 3.0 Base (Confidentia Availability Vector: (CVSS:3.0/A :N/S:U/C:H/ CVE-ID:CVE	sion Middent: Map Beversions the versions the second stacks of the control of the	dleware suilder). hat are .0 and loitable allows er with TTP to Fusion Viewer. of this sult in Fusion r. CVSS 9.8 ity and CVSS			08- 18/153
Hardware Man	agement Pack							
NA	18-07-2018	4.3	Vulnerabili Managemen of Oracle Products (subcomported affected is exploit vulnauthentic network accompromise Managemen attacks of the result in the access to a subcomposite Managemen attacks (Confidential Vector: (CVSS:3.0/AI:N/S:U/C:L.	Sun Sun Sun Sun Sun Version to 11.3. Diffilmerability ated attack seess via Interest of Hat Pack acceptance of Hat	Systems Suite ol). The chat is cult to allows er with PMI to ardware ccessful ility can d read ardware cessible core 3.7 s). CVSS	NA		A-Ora- Hardw/0 1-08- 18/154
CV Scoring Scale (C	VSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

CV Scoring Scale (CVSS)	3-4	4-3	3-0	0-7	7-6	0-9	9-10	
Vulnerability Type(s): CSRF-Cross Site Request Forgery: Dir. Tray -Directory Trayersal: DoS-Denial of Service: NA. Not Applicable:								

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Reference/Patch	NCIIPC ID
- 19 p c (0)			CVE-ID:CVE-2018-2906		
Hospitality Cru	ise Fleet Mana	gement			
Hospitality Ope	18-07-2018	anagem	Vulnerability in the Oracle Hospitality Cruise Fleet Management 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
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 (C	VSS)	3-4	4-5 5-6 6-7	7-8 8-9	9-10
	(s): CSRF-Cross Site	_	orgery; Dir. TravDirectory Traversal; Do	S-Denial of Service; NA- N	ot 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

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
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 C C . L (CVCC)	3-4	4-5	5-6	6-7	7-8	8-9	9-10
CV Scoring Scale (CVSS)							

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID			Reference/	Patch	NCIIPC ID
NA NA	18-07-2018	5	result in a access to a Hospitality Services acc 3.0 Bass (Confidentia Vector: (CVSS:3.0/A:N/S:U/C:L/CVE-ID:CVE-ID	unauthorized subset of OPERA 5 Possible date Score ality impacts (V:N/AC:L/F(I:N/A:N). E-2018-295 ity in the OPERA 5 Pomponent of Appliance is 5.5.x. vulne unauther to composite the network to composite version version to composite version to composite version version version to composite version versio	d read Oracle roperty a. CVSS 5.3 s). CVSS PR:N/UI 5 Oracle roperty Oracle ications ig). The hat is Easily erability nticated access promise PERA 5 ccessful illity can access omplete spitality Services 6.0 Base	NA		A-Ora- Hospi/01- 08- 18/160
			(CVSS:3.0/A:N/S:U/C:H,		,			
Hospitality Sim	phony							
DoS	18-07-2018	6	Vulnerability Hospitality component Hospitality (subcomport Import/Exp versions th 2.8, 2.9 and exploit vu	of Applinent: ort). Sup at are affec d 2.10. Diff	oracle ications oported ted are	NA		A-Ora- Hospi/01- 08- 18/161
CV Scoring Scale (C	VSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	cvss	Descrip	otion & CVE	ID	Reference/	Patch	NCIIPC ID
			deletion or to critical Hospitality accessible unauthorizedata or con Oracle Hospitality accessible unauthorizedata	ccess via He Oracle Hose Successful erability can norized comodification data or all sindata as ved access to aplete access pitality Sindata of OOS) of Simphony. Of T.1 (Confide and Ava CVSS AV:N/AC:H/I/I:H/A:L).	TTP to spitality attacks in result reation, in access Oracle imphony well as critical is to all imphony and cause a service Oracle itySS 3.0 intiality, ilability Vector: PR:L/UI			
Hyperion Data NA	Relationship M 18-07-2018	lanagen 5		ity in the H	yperion	NA		A-Ora-
			Data Management Oracle (subcompore security). version the 11.1.2.4.330 vulnerability unauthentice network accompromise Relationship While the Hyperion Management significantly products. Su this vulnera	t compon Hyment: Acces The sup at is affect D. Easily exp wated attack cess via HT Hyperior Manag vulnerabilit Data Relat at, attacks wimpact adduccessful attacks	yperion ss and pported cted is loitable allows er with CTPS to n Data gement. y is in ionship may ditional tacks of			Hyper/01 -08- 18/162
CV Scoring Scale (C	VSS)	3-4	4-5	5-6	5-6 6-7 7-8 8-9		9-10	

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 Finar			** 1		
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		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	A-Ora- Ilear/01- 08- 18/164	
CV Scoring Scale (C	VSS)	3-4	4-5 5-6 6-7	7-8 8-9	9-10

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 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:30/AV:N/AC:L/PR:N/UI:R/S:C/C:H/EL/A:N). CVE-IDI-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 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	Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Reference/Patch	NCIIPC ID
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				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).		
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		18-07-2018	5		NA	
				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		08-

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
			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-0ra- Istor/01- 08- 18/167

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

Vulnerability Type(s)	Publish Date	cvss	Descrip	otion & CVE	: ID	Reference/	Patch	NCIIPC ID
- J P = (0)			Oracle iS	vulne unauther th network to compare from a the attack vulnerability ore, attack impact ad accessful attackers to aplete access to aplete access to a lete acce	Easily crability naticated access promise ccessful human person are and y is in a may ditional tacks of esult in critical as to all data as update, to some cessible core 8.2 integrity Vector: PR:N/UI			
Jd Edwards Ent	terpriseone Tod	ols						
NA	18-07-2018	4	Vulnerabili Edwards Er component Edwards (subcomponent Runtime). version that Easily explois allows low with netword to comprone EnterpriseO Successful vulnerability unauthorize data or component	of Orac of Orac Paent: The sup t is affected itable vulne privileged a rk access vi mise JD E ne attacks of y can res d access to	cle JD roducts Web ported lis 9.2. erability attacker a HTTP dwards Tools. of this sult in critical	NA		A-Ora- Jd/01-08- 18/168
CV Scoring Scale (C	VSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

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
			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-0ra- 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)	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-0ra- Jd/01-08- 18/171

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
			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-0ra- Jd/01-08- 18/172

CV C C . L (CVCC)	3-4	4-5	5-6	6-7	7-8	8-9	9-10
CV Scoring Scale (CVSS)							

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Reference/Patch	NCIIPC ID
JF - (-)			CVE-ID:CVE-2018-2948		
NA 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). CVS 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 (C		3-4	4-5 5-6 6-7 Forgery; Dir. TravDirectory Traversal; Do	7-8 8-9	9-10

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-0ra- Jd/01-08- 18/175

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

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-0ra- 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)	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/U I:N/S:U/C:H/I:N/A:N).	https://security.netapp.com/advisory/ntap-20180726-0001/	A-Ora- JDK,J/01- 08- 18/178
NA	18-07-2018	4.3	CVE-ID:CVE-2018-2972 Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE	https://security.n etapp.com/adviso ry/ntap-	A-Ora- JDK,J/01- 08-
			(subcomponent: JSSE). Supported versions that are	20180726-0001/,	18/179

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
			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/U I:N/S:U/C:N/I:H/A:N). CVE-ID:CVE-2018-2973	https://access.red hat.com/errata/R HSA-2018:2253, https://access.red hat.com/errata/R HSA-2018:2254, https://access.red hat.com/errata/R HSA-2018:2255, https://access.red hat.com/errata/R HSA-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.red hat.com/errata/R HSA-2018:2255, https://access.red hat.com/errata/R HSA-2018:2256, https://security.n etapp.com/adviso	A-Ora- JDK,J/01- 08- 18/180

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
			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.red hat.com/errata/R HSA-2018:2254, https://access.red hat.com/errata/R HSA-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.red hat.com/errata/R HSA-2018:2256, https://access.red hat.com/errata/R HSA-2018:2253, https://security.n etapp.com/adviso ry/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)	Publish Date	cvss	Descrip	tion & CVE	ID	Reference/	Patch	NCIIPC ID
NA	18-07-2018	5.1	significantly products. Su this vulneral takeover of yulnerability deployments clients runni Web Start sandboxed load and ru (e.g., code the internet) and sandbox for vulnerability Java deployments are deployments. Servers, that trusted compared to the component (CVSS:3.0/A) I:R/S:C/C:H/CVE-ID:CVE Vulnerability Vector: (CVSS:3.0/A) I:R/S:C/C:H/CVE-ID:CVE Vulnerability component (subcomponent (subcompone	the vulneral te, attacks impact addiccessful attacks impact addiccessful attacks impacts. Now applies to applies to application at comes from the accurity does not a ments, typical and and rode (e.g., an administry and administry application application application application application and administry are accurately attacks are accurately attacks.	ditional tacks of esult in te: This to Java ly in ted Java ons or ts, that ed code com the he Java v. This apply to cally in un only code strator). The 8.3 ity and CVSS PR:N/U 4 [ava SE Java SE J	https://accehat.com/err HSA-2018:2 https://accehat.com/err HSA-2018:2 https://secuetapp.com/ary/ntap-20180726-0 https://accehat.com/err	ata/R 256, ess.red ata/R 253, arity.n adviso 0001/,	A-Ora- JDK,J/01- 08- 18/182
			significantly	impact ad	ditional	HSA-2018:2	255,	
CV Scoring Scale (C	VSS) (s): CSRF-Cross Site	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
			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/U I:R/S:C/C:H/I:H/A:H). CVE-ID:CVE-2018-2941	https://access.red hat.com/errata/R HSA-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.n etapp.com/adviso ry/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)	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/U I: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.n etapp.com/adviso ry/ntap- 20180726-0001/	A-Ora- JDK,J/01- 08- 18/184

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
			(Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/U I:N/S:C/C:H/I:H/A:H). CVE-ID:CVE-2018-2938		
JDK,JRE,Jrocki	1			1	
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/U I:N/S:U/C:N/I:N/A:L).	· · · · · · · · · · · · · · · · · · ·	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)	Publish Date	cvss	Descrip	otion & CVE	EID	Reference/	Patch	NCIIPC ID
1966			CVE-ID:CVE	-2018-295	2			
Marketing					\			
NA	18-07-2018	4	Marketing Oracle E (subcompor Supported affected ar 12.1.3, 12.2 12.2.6 and exploit vu unauthentic network ac compromise Successful human int person othe and while t in Oracle I may sign additional p attacks of th result in ur to critical access to al accessible unauthorize delete acces Marketing CVSS 3.0 (Confidential impacts). (CVSS:3.0/A I:R/S:C/C:H, CVE-ID:CVE	Horacle Marketing, authorized data or coll oracle Marketing, authorized data as well authorized data or coll oracle Marketing, authorized data as well authorized data as well authorized data or coll oracle Marketing, authorized data as well authorized data. Some of accessible Base Scoolity and Inc. CVSS V:N/AC:H/II.L/A:N). 1-2018-298	nt of Suite oducts). hat are 12.1.2, 12.2.5, ficult to allows ter with TTP to rketing. require from a attacker bility is attacks impact ccessful ility can access omplete arketing well as insert or f Oracle data. ore 6.9 integrity Vector: PR:N/U	NA		A-Ora- Marke/01 -08- 18/185
NA	18-07-2018	5.8	Marketing	Supported vared to the state of	nt of Suite User versions 12.1.1, Easily erability	NA		A-Ora- Marke/01 -08- 18/186
CV Scoring Scale (CV	VSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	cvss	Descrip	otion & CVE	ID I	Reference/	Patch	NCIIPC ID
			attacker wivia HTTP Oracle Manattacks interaction other than while the Oracle Manaignificantly products. So this vulnera unauthorize data or com Oracle Manattacks interaction other than while the Oracle Manattacks interaction oracle Manattacks interaction other than while the Oracle Manattacks interaction oracle Manattack data as we update, insert to some of accessible di Score 8.2 (Integrity Vector: (CVSS:3.0/A :R/S:C/C:H/	to composite to composite the attack vulnerability cattack vulnerability cattack vulnerability cattack to accessful attacked access to aplete access the access to aplete access the access to access the access to access the access to access to access the access to access the access the access the access the access the access to access the access the access to access the access the access to access the access the access to access the access the access to access the access to access the access to access	bromise ccessful human person ter and y is in eks may ditional tacks of esult in critical es to all cessible horized e access arketing 8.0 Base dity and CVSS			
Micros Relate (Managemen	t Software				
DoS	18-07-2018	5.5	Relate component Applications Internal Supported affected are Easily exploallows low with network to comprom CRM Softwulnerability Relate CRM	of Oracle s (subcom Oper versions the 10.8.x and itable vulne privileged ark access vinise MICROS ware. While Software, inficantly products. Such authorized	oftware Retail ponent: rations). nat are 11.4.x. erability attacker a HTTP S Relate le the MICROS attacks impact ccessful ility can update,	NA	(A-Ora- Micro/01- 08- 18/187
CV Scoring Scale (C	VSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

		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		
18-07-2018	3.7	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
	8-07-2018		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 8-07-2018 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	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 8-07-2018 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

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
			6.7 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:P/AC:H/PR:H/U I: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) 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	0 =	
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
NA 18-07-2018	3.5	Vulnerability in the MySQL https://security.n A-Ora-Server component of Oracle etapp.com/adviso 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.n etapp.com/adviso ry/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)	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.n etapp.com/adviso ry/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.n etapp.com/adviso ry/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)	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.n etapp.com/adviso ry/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.n etapp.com/adviso ry/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)	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.n etapp.com/adviso ry/ntap- 20180726-0002/	A-0ra- 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.n etapp.com/adviso ry/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)	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.n etapp.com/adviso ry/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.n etapp.com/adviso ry/ntap- 20180726-0002/	A-0ra- 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)	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.n etapp.com/adviso ry/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.n etapp.com/adviso ry/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)	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.n etapp.com/adviso ry/ntap- 20180726-0002/	A-0ra- 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.n etapp.com/adviso ry/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)	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.n etapp.com/adviso ry/ntap- 20180726-0002/	A-0ra- 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.n etapp.com/adviso ry/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
9 ()							

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.n etapp.com/adviso ry/ntap- 20180726-0002/	A-0ra- 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.n etapp.com/adviso ry/ntap- 20180726-0002/	A-0ra- 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)	Publish Date	cvss	Description & CVE ID	Reference/Patch	NCIIPC ID
NA 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/U I:N/S:U/C:N/I:L/A:H). CVE-ID:CVE-2018-3081	https://security.n etapp.com/adviso ry/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.n etapp.com/adviso ry/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)	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/U I: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		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.n etapp.com/adviso ry/ntap- 20180726-0002/	A-0ra- 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)	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 Workber					
One-to-one Ful	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/U I:N/S:U/C:L/I:N/A:N). CVE-ID:CVE-2018-2598		A-Ora- Mysql/01 -08- 18/214

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

Vulnerability Type(s)	Publish Date	cvss	Descrip	otion & CVE	: ID	Reference/	Patch	NCIIPC ID
NA	18-07-2018	5.8	Vulnerabilione-to-One component Business (subcomported affected ar 12.1.3, 12.2 12.2.6 and exploitable allows attacker wivia HTTP Oracle One-Successful human interpretation of the and while the in Oracle One-to-One accessible unauthorized data or com Oracle One-accessible unauthorized delete accessible delete accessible deleteration (CVSS:3.0/A:R/S:C/C:H/CVE-ID:CVE	of Oraclent: Print Sections the 12.1.1, 2.3, 12.2.4, d 12.2.7. vulne unauther the network to compete attacks eraction for than the adhe vulnerable one attacks impact addiccessful attacks impact addiccessful attacks to oplete access to oplete ac	fillment cle E-Suite Server). hat are 12.1.2, 12.2.5, Easily erability inticated access bromise fillment. require from a hattacker bility is -to-One may ditional tacks of esult in critical as to all fillment well as insert or foracle fillment c.0 Base lity and CVSS	NA		A-Ora- One-t/01- 08- 18/215
Order Manage NA	18-07-2018	4.4	Vulnerahili	ty in the	Oracle	NA		A-Ora-
	2007 2010		Order Mana	gement con	ponent			Order/01
			of Oracle					-08- 19/216
			(subcompor Diagnostic		Product			18/216
			versions that					
CV Scoring Scale (C	VSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10

CV Scoring Scale (CVSS)

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

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 Tech	hnology				
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 In Technology. Note: Outside	NA	A-0ra- Outsi/01- 08- 18/217
		3-4	4-5 5-6 6-7	7-8 8-9	9-10

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
			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)	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)	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 In Technology.	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)	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 In Technology.	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)	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 In Technology.	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)	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 In Technology.	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)	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 In Technology.	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)	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)	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 In Technology.	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)	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 In Technology.	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)	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 In Technology.	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)	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 In Technology.	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)	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 In Technology.	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
9 ()							

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		
	erprise Cs Finar				1
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)	Publish Date	cvss	Description & CVE I	ID	Reference/P	atch	NCIIPC ID
	erprise Human	Capital	Management Human Res	sources			
NA	18-07-2018	5.8	Vulnerability in PeopleSoft Enterprise Human Resources compof Oracle PeopleSoft Pro(subcomponent: Compensation). The support version that is affected Easily exploitable vulnerallows unauthent attacker with network avia HTTP to compropeopleSoft Enterprise Human Resources. Succeptattacks require interaction from a pother than the attacker while the vulnerability PeopleSoft Enterprise Human Resources, attack significantly impact additionally products. Successful attact this vulnerability can resunauthorized update, insidelete access to som PeopleSoft Enterprise Human Resources acceptated as well as unauthorized access to a subsepeopleSoft Enterprise Human Resources acceptated access to a subsepeopleSoft Enterprise Human	the HCM conent oducts ported is 9.2. rability ticated access romise HCM cessful numan person er and is in HCM as may itional acks of sult in sert or ne of HCM essible orized set of HCM ressible orized set of HC	NA		A-Ora- Peopl/01- 08- 18/232
Peoplesoft Ente	erprise Peoplet	ools		1			
NA	18-07-2018	4	PeopleTools component Oracle PeopleSoft Pro (subcomponent: PIA S	oducts	NA		A-Ora- Peopl/01- 08- 18/233
CV Scoring Scale (C	VSS)	3-4	4-5 5-6	6-7	7-8	8-9	9-10
Vulnerability Type(orgery; Dir. TravDirectory Trav	versal; Dos	S-Denial of Service	e; NA- No	ot 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

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

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

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

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/U I: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

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
			(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)	Publish Date	cvss	Descrip	otion & CVE	: ID	Reference/	Patch	NCIIPC ID
			Supported affected are Easily exploallows attacker wivia HTTP PeopleSoft PeopleTools attacks interaction other than while the PeopleSoft PeopleTools significantly products. Support of the Support of the PeopleSoft PeopleTools well as unauthorized delete accepted as unauthorized access to PeopleSoft PeopleTools well as unaccess to PeopleSoft PeopleTools CVSS 3.0 (Confidential impacts). (CVSS:3.0/A:R/S:C/C:L/CVE-ID:CVE	e 8.55 and itable vulner unauther the network to compare from a the attack vulnerability. Enter the attack vulnerability can reducessful attacks impact addiccessful attacks in the attack vulnerability can reduces to so Enter accessible nauthorized a substance a substanc	d 8.56. erability nticated access bromise terprise ccessful human person ter and y is in terprise may ditional tacks of esult in nsert or ome of terprise data as d read set of terprise e data. re 6.1 ntegrity Vector: PR:N/UI			
Peoplesoft Hun	nan Resource M	lanaaem	ent Systems					
NA	18-07-2018	5	Vulnerabili PeopleSoft of Oracle Person (subcomport Gateway). version that Easily exploit allows attacker wirespectives.	ty in HRMS comeopleSoft Pent: Ca The superior substitution is affected itable vulne unauther to compound HRMS. Superior subseption is superior substitution.	roducts ndidate pported l is 9.2. erability nticated access oromise ccessful	NA		A-Ora- Peopl/01- 08- 18/241
CV Scoring Scale (C	VSS)	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
Duine group DC	Enterprise Proj	act Povit	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		
NA	18-07-2018	ect Port	folio Management Vulnerability in the	NA	A-Ora-
IVA	18-07-2018	3.0	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.	INA	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)	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 C C . L (CVCC)	3-4	4-5	5-6	6-7	7-8	8-9	9-10
CV Scoring Scale (CVSS)							

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

|--|

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 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). CVF-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 16x. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise 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 impacts).	Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Reference/Patch	NCIIPC ID
NA 18-07-2018 Vulnerability in the Prima/01 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:				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).		
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:	Primavera Uni	fier				
	NA	18-07-2018	4	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:	NA	Prima/01 -08-

or seering some (cross)	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
			: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
9 ()							

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)	Publish Date	cvss	Description & CVE ID	NCIIPC ID	
19000			CVE-ID:CVE-2018-2965		
Retail Bulk Date	a Integration				
NA	18-07-2018	5.8 And Seg. 5.5	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 accessiva 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/US:R/S:C/C:L/I:L/A:N). CVE-ID:CVE-2018-2891 Imentation Foundation Vulnerability in the Oracle Retail Customer Management and Segmentation Foundation	NA NA	A-Ora-Retai/01-08-18/250 A-Ora-Retai/01-08-
			and Segmentation Foundation component of Oracle Retail Applications (subcomponent Internal Operations)	08- 18/251	
CV Scoring Scale (CV	(SS)	3-4	4-5 5-6 6-7	7-8 8-9	9-10
	-	Request F	orgery; Dir. TravDirectory Traversal; I	OoS-Denial of Service; NA- N	ot Applicable;

Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	cvss		Descrip	otion & CVE	ID	Reference/	Patch	N	CIIPC ID
			affect Easil allow with to c Cust Segn Whill Orac Man Segn attac impa Succ vuln unau delet Reta and acce unau parti (par Cust Segn (CVS) (Inte	tted are ly explosed in explosion explosion explosion explosed in explosion explosio	vulnerabilit letail Cu t in Four hay signi ditional pr attacks co y can res d update, ir s to some o omer Mana htation Fou data d ability to nial of S) of Oracle Managemer Base Sco	d 17.x. erability attacker a HTTP e Retail at and adation. y is in astomer and adation, ficantly roducts. of this sult in asert or f Oracle gement and cause a service e Retail at and adation. re 6.4 ilability Vector: PR:L/UI				
Scripting	L		0.2							
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				Sc:	-0ra- rip/01- }- 8/252		
CV Scoring Scale (C	VSS)	3-4		4-5	5-6	6-7	7-8	8-9		9-10

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

Vulnerability Type(s)	Publish Date	cvss	Descrip	otion & CVE	EID	Reference/	Patch	NCIIPC ID
			attacks interaction other than while the Oracle Scrip significantly products. So this vulnera unauthorize data or con	the attack vulnerability of the pring, attack impact addiccessful attack in the principal of the principal o	human person ser and y is in ks may ditional tacks of esult in critical ss to all cessible chorized e access cripting 8.0 Base lity and CVSS			
Siebel Ui Fram		ı						
NA	18-07-2018	4.3	Framework Oracle (subcomporaffected exploitable allows attacker wind wind response)	Siebel nent: UIF Opted version is 18.0. vulne unauther th network to comp UI Fran attacks reraction for than the a attacks of y can resed update, in st to some cork accessib	ent of CRM pen UI). that is Easily erability e	NA		A-Ora- Siebe/01- 08- 18/253
CV Scoring Scale (C		3-4	4-5	5-6	6-7	7-8	8-9	9-10

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			
			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-0ra- Soa/01- 08- 18/254			
Solaris Cluster				1	A-Ora-			
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	alnerability in the Solaris ster component of Oracle Systems Products Suite becomponent: NAS device dition). Supported versions at are affected are 3.3 and Easily exploitable nerability allows authenticated attacker with twork access via RPC to impromise Solaris Cluster. Eccessful attacks of this increability can result in the sever of Solaris Cluster. SS 3.0 Base Score 9.8				
CV Scoring Scale (C		3-4	4-5 5-6 6-7 Torgery; Dir. TravDirectory Traversal; Do	7-8 8-9	9-10			

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 Manager	ment				
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-0ra- Trade/01 -08- 18/256
NA	18-07-2018	5.8	Vulnerability in the Oracle Trade Management	NA	A-Ora- Trade/01

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

Vulnerability Type(s)	Publish Date	cvss	Descrip	Patch	NCIIPC ID			
			component Business (subcomponent Business (subcomponent Interface). Subcomponent Interface). Subcomponent Interface). Subcomponent Interface). Subcomponent Interface). Subcomponent Interface Inter	-08- 18/257				
Tuxedo			CVE IDICVE	2010 501				
NA	18-07-2018	5	Tuxedo cor Fusion (subcompor Supported affected are	Midonent: versions the 12.1.1, 12. asily exp	Oracle dleware Core). nat are 1.3 and loitable allows	NA		A-0ra- Tuxed/01 -08- 18/258
CV Scoring Scale (C	VSS)	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
			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		
NA 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
		2.4	subset of Oracle VM VirtualBox	7.0	

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
			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

CV C C . L (CVCC)	3-4	4-5	5-6	6-7	7-8	8-9	9-10
CV Scoring Scale (CVSS)							

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

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
			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-0ra- Vm/01- 08- 18/264

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

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

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
			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 Por					,
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/0 1-08- 18/266
Weblogic Serve	er				
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 (C	VSS)	3-4	4-5 5-6 6-7	7-8 8-9	9-10
Vulnerability Type	(s): CSRF-Cross Site	Request F	orgery; Dir. TravDirectory Traversal; Do	S-Denial of Service; NA- N	ot Applicable;

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Reference/Patch	NCIIPC ID
Τγρο(δ)			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

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
			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-0ra- 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)	Publish Date	cvss	Description & CVE ID	Reference/Patch	NCIIPC ID
VF - (-)			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-0ra- Weblo/01 -08- 18/271

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

le Token Pro l <mark>e Token</mark> 09-07-2018	oject 5	The mintToken function of smart contract implementate for Orderbook Presale Toll (OBP), an Ethereum token, an integer overflow that allot the owner of the contract to the balance of an arbitr user to any value. CVE-ID:CVE-2018-13676	m/BlockChainsSec ken urity/EtherTokens has /tree/master/Pres ows aleToken, set	A-Ord- Order/01 -08- 18/272
le Token		smart contract implementate for Orderbook Presale Tol (OBP), an Ethereum token, an integer overflow that allot the owner of the contract to the balance of an arbitruser to any value.	m/BlockChainsSec ken urity/EtherTokens has /tree/master/Pres aleToken, set ary https://github.co	Order/01 -08-
	5	smart contract implementate for Orderbook Presale Tol (OBP), an Ethereum token, an integer overflow that allot the owner of the contract to the balance of an arbitruser to any value.	m/BlockChainsSec ken urity/EtherTokens has /tree/master/Pres aleToken, set ary https://github.co	Order/01 -08-
09-07-2018	5	smart contract implementate for Orderbook Presale Tol (OBP), an Ethereum token, an integer overflow that allot the owner of the contract to the balance of an arbitruser to any value.	m/BlockChainsSec ken urity/EtherTokens has /tree/master/Pres aleToken, set ary https://github.co	Order/01 -08-
			urity/EtherTokens /blob/master/GE MCHAIN/mint%2 0integer%20overf low.md	
ect				
09-07-2018	5		m/BlockChainsSec eum urity/EtherTokens low /blob/master/GE the MCHAIN/mint%2 e of Ointeger%20overf	A-Ota- Otaku/01 -08- 18/273
oject				
09-07-2018	5	smart contract implementat for PELOCoinToken, Ethereum token, has an inte overflow that allows the ow of the contract to set	m/BlockChainsSec urity/EtherTokens ger /tree/master/PEL oCoinToken,	A-Pel- Peloc/01- 08- 18/274
-	3-4			9-10
		-07-2018 5	contract to set the balance an arbitrary user to any va CVE-ID:CVE-2018-13755 The mintToken function of smart contract implementate for PELOCoinToken, Ethereum token, has an interpretation of the contract to set balance of an arbitrary user any value.	contract to set the balance of an arbitrary user to any value. CVE-ID:CVE-2018-13755 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 CVE-ID:CVE-2018-13738 CVE-ID:CVE-2018-13738 CVE-ID:CVE-2018-13738 CVE-ID:CVE-2018-13738 CVE-ID:CVE-2018-13738 Ointeger%20overf low.md, https://github.co m/BlockChainsSec urity/EtherTokens /tree/master/PEL OCoinToken, https://github.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Reference/	Patch	NCIIPC ID
				0integer%20 low.md	Ooverf	
Play2liveprom	o Project			·	·	
Play2liveprom						
Overflow	09-07-2018	5	The mintTokens function of smart contract implementation for Play2LivePromo, as Ethereum token, has an integoverflow that allows the own of the contract to set the balance of an arbitrary user any value. CVE-ID:CVE-2018-13698	on m/BlockCha an urity/EtherT ger /tree/maste ter 2LivePromo, he	insSec Tokens r/Play ub.co insSec Tokens er/GE nt%2	A-Pla- Play2/01- 08- 18/275
Pmet Project						
Pmet						
Overflow	09-07-2018	5	The mintToken function of smart contract implementation for PMET, an Ethereum toke has an integer overflow the allows the owner of the contract to set the balance an arbitrary user to any value CVE-ID:CVE-2018-13712	on m/BlockCha en, urity/EtherT nat /tree/maste he ET, of	insSec Tokens r/PM ub.co insSec Tokens er/GE nt%2	A-Pme- Pmet/01- 08- 18/276
Pmhtoken Pro	ject					
Pmhtoken						
Overflow	09-07-2018	5	The mintToken function of smart contract implementation for PMHToken, an Ethereu token, has an integer overflow that allows the owner of the contract to set the balance an arbitrary user to any value CVE-ID:CVE-2018-13705	on m/BlockCha um urity/EtherT ow /tree/maste he HToken, of	insSec Tokens r/PM ub.co insSec Tokens	A-Pmh- Pmhto/0 1-08- 18/277
CV Scoring Scale (C	VSS)	3-4	4-5 5-6 6	6-7 7-8	8-9	9-10
		Request F	orgery; Dir. TravDirectory Traversal	l; DoS-Denial of Servi	ce; NA- Not	t Applicable;

Vulnerability Type(s)	Publish Date	cvss	Descrip	tion & CVE	ID	Reference/	'Patch	NCIIPC ID		
						MCHAIN/mi 0integer%2 low.md				
Projectj Projec	:t									
Projectj										
Overflow	09-07-2018 5		smart contra for Project token, has a that allows contract to an arbitrary	art contract implementation ProjectJ, an Ethereum ten, has an integer overflow at allows the owner of the attract to set the balance of arbitrary user to any value.		https://gith m/BlockCha urity/Ether/ /tree/maste ectJ, https://gith	insSec Tokens er/Proj ub.co	A-Pro- Proje/01- 08- 18/278		
			CVE-ID:CVE	-2018-13/	33	m/BlockCha urity/Ether? /blob/maste MCHAIN/mi Ointeger%20 low.md	Fokens er/GE int%2			
Rckt Coin Project										
Rckt Coin	T									
Overflow	09-07-2018	5	The mintT smart contrator RCKT_C token, has a that allows contract to an arbitrary CVE-ID:CVE	oin, an Et n integer o the owner set the bal user to an	entation hereum verflow of the ance of y value.	https://gith m/BlockCha urity/Ether?/blob/maste MCHAIN/mi Ointeger%20 low.md, https://gith m/BlockCha urity/Ether?/tree/maste	insSec Fokens er/GE int%2 Ooverf ub.co insSec Fokens	A-Rck- Rckt/01- 08- 18/279		
Dodtialest Desi	o at					T_Coin				
Redticket Proj Redticket	CCL									
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.		https://gith m/BlockCha urity/Ether? /tree/maste Ticket, https://gith	insSec Tokens er/Red ub.co	A-Red- Redti/01- 08- 18/280			
			CVE-ID:CVE-2018-13696			m/BlockCha urity/Ether				
CV Scoring Scale (C	VSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10		
	ulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. TravDirectory Traversal; DoS-Denial of Service; NA- Not Applicable; ql-SQL Injection; XSS- Cross Site Scripting;									

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Reference/Patch	NCIIPC ID
				/blob/master/GE MCHAIN/mint%2 0integer%20overf low.md	
Richiumtoken	Project				
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.co m/BlockChainsSec urity/EtherTokens /tree/master/Rich iumToken, https://github.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 Ointeger%20overf low.md	A-Ric- Richi/01- 08- 18/281
Riptidecoin Pr	oject				
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.co m/BlockChainsSec urity/EtherTokens /tree/master/Ript ideCoin, https://github.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 Ointeger%20overf low.md	A-Rip- Ripti/01- 08- 18/282
Robotbtc Proje	ect				
Robotbtc					

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

Vulnerability Type(s)	Publish Date	cvss	Descrip	tion & 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://gith m/BlockCha urity/Ether' /tree/maste otBTC, https://gith m/BlockCha urity/Ether' /blob/maste MCHAIN/m Ointeger%2 low.md	ninsSec Fokens er/Rob ub.co ninsSec Fokens er/GE int%2	A-Rob- Robot/01 -08- 18/283			
Rocket Coin Project										
Overflow	12-07-2018	5	vulnerability function r	exists multiTransf pin (XRC token attacker co	smart smart ould use oalance.	https://gith m/VenusAD therTokens, master/Roc 0Coin%28X 9, https://gith m/VenusAD therTokens, master/SHA CH/SHARKT	Lab/E /tree/ ket%2 RC%2 ub.co Lab/E /blob/ LRKTE	A-Roc- Rocke/01 -08- 18/284		
Rrtoken Projec	ct									
Rrtoken	00.07.5515			1 2		, , , , ,	, ,			
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://gith m/BlockCha urity/Ether' /blob/maste MCHAIN/m Ointeger%2 low.md, https://gith m/BlockCha urity/Ether' /tree/maste	ninsSec Fokens er/GE int%2 Ooverf ub.co ninsSec Fokens	A-Rrt- Rrtok/01- 08- 18/285			
Dr. L. C. D.						oken	.1 / IUI			
Rtokenmain P	roject									
CV Scoring Scale (C		3-4	4-5	5-6	6-7	7-8	8-9	9-10		
Vulnerability Type	ulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. TravDirectory Traversal; DoS-Denial of Service; NA- Not Applicab						ot 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.co m/BlockChainsSec urity/EtherTokens /tree/master/RTo kenMain, https://github.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 0integer%20overf low.md	-08- 18/286
Servviziotoker	ı Project				
Servviziotoken	<u>, </u>			,	
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	08- 18/287
Sexhdsolo Pro	ject				
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	-08- 18/288
CV Scoring Scale (C	VCC)	3-4	4-5 5-6 6-7	7-8 8-	9 9-10
Vulnerability Type(orgery; Dir. TravDirectory Traversal; D	oS-Denial of Service; NA-	Not Applicable;

 ${\bf Sql\text{-}SQL\ Injection;\ XSS\text{-}\ Cross\ Site\ Scripting;}$

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Reference/Patch	NCIIPC ID					
Sharktech Pro	ject									
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.co m/VenusADLab/E therTokens/blob/ master/SHARKTE CH/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.co m/BlockChainsSec urity/EtherTokens /tree/master/SOS Coin, https://github.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 Ointeger%20overf low.md	A-Sos- Sosco/01- 08- 18/290					
Stctoken Proje	ct									
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.co m/BlockChainsSec urity/EtherTokens /tree/master/STC Token, https://github.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 Ointeger%20overf low.md	A-Stc- Stcto/01- 08- 18/291					
Superenergy P	roject									
Superenergy										

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

Vulnerability Type(s)	Publish Date	cvss	Descrip	otion & CVE	: ID	Reference/	'Patch	NCIIPC ID
Overflow	09-07-2018	5	smart contr	Energy (SE oken, has an at allows the ntract to s an arbitrary	entation (C), an integer e owner set the user to	https://githm/BlockChaurity/Ether/Intree/mastern/BlockChaurity/Ether/Introduced/blob/mastern/Blo	ninsSec Tokens er/SEC, ub.co ninsSec Tokens er/GE int%2	A-Sup- Super/01 -08- 18/292
Theflashtoken	shtoken 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://githm/BlockChaurity/Ether?/blob/maste/MCHAIN/mi/Ointeger%20low.md, https://githm/BlockChaurity/Ether?/tree/maste/FlashToken	insSec Fokens er/GE int%2 Ooverf ub.co insSec Fokens	A-The- Thefl/01- 08- 18/293
Thread Project	t							
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.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 Ointeger%20overf low.md, https://github.co m/BlockChainsSec urity/EtherTokens /tree/master/Thr ead		A-Thr- Threa/01 -08- 18/294	
Tickets Project	t							
Tickets								
CV Scoring Scale (CV	VSS)	3-4	4-5 5-6 6-7		7-8	8-9	9-10	

Vulnerability Type(s)	Publish Date	cvss	Descrip	tion & 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://githm/BlockChaurity/Etherdets, https://githm/BlockChaurity/Etherdets/blob/mastMCHAIN/mOinteger%2low.md	ninsSec Tokens er/tick ub.co ninsSec Tokens er/GE int%2	A-Tic- Ticke/01- 08- 18/295
Tokenmachu F	Project							
Tokenmachu Overflow	09-07-2018	5	The mintTo			https://gith		A-Tok-
			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			m/BlockCha urity/Ether' /blob/mast MCHAIN/m 0integer%2 low.md,	Tokens er/GE int%2	Token/01 -08- 18/296
			•	any value. CVE-ID:CVE-2018-13731			https://github.co m/BlockChainsSec urity/EtherTokens /tree/master/Tok enMACHU	
Tradesman Pr	oject							
Tradesman	,							
Overflow	09-07-2018	5	The mintTo smart contra for Tradesn token, has a that allows contract to an arbitrary	nct implemen nan, an Et n integer o the owner set the bal	entation hereum verflow of the ance of	https://githm/BlockChaurity/Ether/tree/mastedesman,https://gith	ainsSec Tokens er/Tra	A-Tra- Trade/01 -08- 18/297
Tubo Duoingt			CVE-ID:CVE-2018-13713 m/BlockChain urity/EtherTol /blob/master/ MCHAIN/mint 0integer%20o low.md			ninsSec Tokens er/GE int%2		
Tube Project								
CV Scoring Scale (C	VSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type	ulnerability Type(s): CSRF-Cross Site		orgery; Dir. Trav	Directory Tr	aversal; Do	S-Denial of Serv	ice; NA- No	ot 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	m/BlockChainsSec urity/EtherTokens /tree/master/Tub e,	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	m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 Ointeger%20overf	A-Ubl- Ublas/01- 08- 18/299					
Ultimatecoin P	roject									
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	m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 0integer%20overf	A-Ult- Ultim/01- 08- 18/300					
CV Scoring Scale (C	VSS)	3-4	4-5 5-6 6-7	7-8 8-9	9-10					
		Request F	orgery; Dir. TravDirectory Traversal; E	oS-Denial of Service; NA- N	ot Applicable;					

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Reference/Patch	NCIIPC ID
Utbtokentest P	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	m/BlockChainsSec urity/EtherTokens /tree/master/UTB TokenTest,	A-Utb- Utbto/01- 08- 18/301
Vanminhcoin I	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	m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2	A-Van- Vanmi/01 -08- 18/302
Vitemoneycoir	n 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 The mintToken function of a https://github.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 Ointeger%20overf		A-Vit- Vitem/01 -08- 18/303
CV Scoring Scale (CV	VSS)	3-4	4-5 5-6 6-7	7-8 8-9	9-10
		Request F	orgery; Dir. TravDirectory Traversal; D	oS-Denial of Service: NA- No	ot Applicable:

Vulnerability Type(s)	Publish Date	cvss	Descrip	tion & CVE	E ID	Reference/	'Patch	NCIIPC ID
						low.md		
Vornoxcointok								
Vornoxcointoke		_	T					
Overflow	09-07-2018	5	The mintTo smart contra for Vornox Name: Vorn Ethereum to overflow that of the conbalance of any value. CVE-ID:CVE	oct implement (VRX) (Octobro) I coxCoinToken, has an and tallows the tract to a second contract. It is a second contract	entation Contract en), an integer e owner set the user to	https://githem/BlockChaurity/Ether/l/tree/masten/blockChaurity/Ether/l/blob/masten/blob/masten/blob/masten/blob/masten/blow.md	ub.co insSec Tokens er/Coi ub.co insSec Tokens er/GE int%2	A-Vor- Vorno/01 -08- 18/304
Wemediachain	Project							
Wemediachain			1					
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://githmyvenusAD therTokens/ master/WeM hain%28WM 9, https://githmyvenusAD therTokens/ master/SHA CH/SHARKT md	Lab/E /tree/ MediaC MC%2 ub.co Lab/E /blob/ RKTE	A-Wem- Wemed/0 1-08- 18/305	
Worldopction	•							
Worldopctionc Overflow	hain 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 The mintToken function of a https://github.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2		A-Wor- World/01 -08- 18/306			
CV Scoring Scale (CV	VSS)	3-4	4-5	5-6	6-7	7-8	8-9	9-10
CV Scoring Scale (CV Vulnerability Type(

Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Reference/Patch	NCIIPC ID					
				0integer%20overf low.md						
Yambyo Projec	t									
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	m/BlockChainsSec urity/EtherTokens /tree/master/YA MBYO,	A-Yam- Yamby/0 1-08- 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	m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 0integer%20overf	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	m/BlockChainsSec urity/EtherTokens /tree/master/YSS, https://github.co	A-Yss- YSS/01- 08- 18/309					
CV Scoring Scale (CV	/SS)	3-4	4-5 5-6 6-7	7-8 8-9	9-10					
		Request F	orgery; Dir. TravDirectory Traversal; [OoS-Denial of Service; NA- N	ot Applicable;					

Sql-SQL Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Reference/Patch	NCIIPC ID
71 ()				0integer%20overf low.md	
Yumerium Pro	ject				
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.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 0integer%20overf low.md https://github.co	A-Yum- Yumer/0 1-08- 18/310
				m/BlockChainsSec urity/EtherTokens /tree/master/Yu merium	
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.co m/BlockChainsSec urity/EtherTokens /tree/master/ZIP, https://github.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 Ointeger%20overf low.md	A-Zip- ZIP/01- 08- 18/311
Zpecoin Projec	:t				
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.co m/BlockChainsSec urity/EtherTokens /tree/master/ZPE coin, https://github.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2	A-Zpe- Zpeco/01 -08- 18/312
CV Scoring Scale (CV	(/SS)	3-4	4-5 5-6 6-7	7-8 8-9	9-10
CV Scoring Scale (C)	/ 33 J				

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Reference/Patch	NCIIPC ID
				0integer%20overf low.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.co m/BlockChainsSec urity/EtherTokens /blob/master/GE MCHAIN/mint%2 0integer%20overf low.md, https://github.co m/BlockChainsSec	A-Zto- Ztoke/01- 08- 18/313
				urity/EtherTokens /tree/master/ZTo	
				ken	
ADM			Hardware		
ARM,Intel					
	rtex-a,Cortex-r,		eron J,Celeron N,Core I3,Core I n J,Pentium N,Xeon,Xeon Bronze		
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
0 1			Operating System (OS)		
Oracle					
Solaris	10.07.0010	4.0	W 1 1 1 1 2 2 2 3 3 3 3 3 3 3 3 3 3 3 3 3	NA	0.0
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	0-0ra- Solar/01- 08- 18/315	
CV Scoring Scale (CV	VSS)	3-4	4-5 5-6 6-7	7-8 8-9	9-10
	(s): CSRF-Cross Site	_	orgery; Dir. TravDirectory Traversal; Do	oS-Denial of Service; NA- No	ot Applicable;

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/U I: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	0-0ra- 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	0-0ra- Solar/01- 08- 18/317

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
			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	0-0ra- 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	0-0ra- Solar/01- 08- 18/319

CV C C . L (CVCC)	3-4	4-5	5-6	6-7	7-8	8-9	9-10
CV Scoring Scale (CVSS)							

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	0-0ra- Solar/01- 08- 18/320

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

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