Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
Application					
Catfish-cms					
Catfish Blog					
CSRF	29-10-2018	**6.8**	A CSRF issue was discovered in admin/Index/tiquan in catfish blog 2.0.33. **CVE-ID:CVE-2018-18735**	https://github.com/AvaterXXX/catfish/blob/master/catfishblog.md#csrf	A-Cat-Catfi/19-11-18/1
Catfish Cms					
CSRF	29-10-2018	**6.8**	A CSRF issue was discovered in admin/Index/addmanageuser.html in Catfish CMS 4.8.30. **CVE-ID:CVE-2018-18734**	https://github.com/AvaterXXX/catfish/blob/master/catfishcms.md#csrf	A-Cat-Catfi/19-11-18/2
IBM					
Rational Quality Manager					
XSS	02-11-2018	**3.5**	IBM Quality Manager (RQM) 5.0 through 5.0.2 and 6.0 through 6.0.6 are vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 132929. **CVE-ID:CVE-2017-1609**	https://exchange.xforce.ibmcloud.com/vulnerabilities/132929	A-IBM-Ratio/19-11-18/3
Websphere Commerce					
XSS	24-10-2018	**3.5**	IBM WebSphere Commerce Enterprise V7, V8, and V9 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 142596. **CVE-ID:CVE-2018-1541**	https://exchange.xforce.ibmcloud.com/vulnerabilities/142596 https://www.ibm.com/support/docview.wss?uid=ibm10731225	A-IBM-Websp/19-11-18/4

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
Oracle					
JDK,JRE					
NA	16-10-2018	**4.3**	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: Utility). The supported version that is affected is Java SE: 11. 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 update, insert or delete access to some of Java SE accessible data. Note: This vulnerability applies to Java deployments 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 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE-ID:CVE-2018-3150**	https://usn.ubuntu.com/3804-1/ https://security.netapp.com/advisory/ntap-20181018-0001/ https://access.redhat.com/errata/RHSA-2018:3521	A-Ora-JDK,J/19-11-18/5
Mysql					
NA	16-10-2018	**4**	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.6.41 and prior, 5.7.23 and prior and 8.0.12 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to	https://usn.ubuntu.com/3799-1/ https://security.netapp.com/advisory/ntap-20181018-0002/ https://lists.debian.org/debian-lts-	A-Ora-Mysql/19-11-18/6

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			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-2018-3143**	announce/2018/11/msg00007.html	
NA	16-10-2018	**4**	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.6.41 and prior, 5.7.23 and prior and 8.0.12 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-2018-3156**	https://usn.ubuntu.com/3799-1/ https://security.netapp.com/advisory/ntap-20181018-0002/ https://lists.debian.org/debian-lts-announce/2018/11/msg00007.html	A-Ora-Mysql/19-11-18/7
NA	16-10-2018	**4**	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.6.41 and prior, 5.7.23 and prior and 8.0.12 and prior. Easily exploitable vulnerability allows low	https://usn.ubuntu.com/3799-1/ https://security.netapp.com/advisory/ntap-20181018-0002/	A-Ora-Mysql/19-11-18/8

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			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-2018-3251**	https://lists.debian.org/debian-lts-announce/2018/11/msg00007.html	
NA	16-10-2018	**4**	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Parser). Supported versions that are affected are 5.5.61 and prior, 5.6.41 and prior, 5.7.23 and prior and 8.0.12 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-2018-3133**	https://lists.debian.org/debian-lts-announce/2018/11/msg00004.html https://security.netapp.com/advisory/ntap-20181018-0002/ https://usn.ubuntu.com/3799-1/ https://usn.ubuntu.com/3799-2/	A-Ora-Mysql/19-11-18/9
NA	16-10-2018	**4**	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Storage Engines). Supported versions that are affected are 5.5.61 and prior, 5.6.41 and prior,	https://lists.debian.org/debian-lts-announce/2018/11/msg00004.html https://lists.debia	A-Ora-Mysql/19-11-18/10

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			5.7.23 and prior and 8.0.12 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-2018-3282**	n.org/debian-lts-announce/2018/11/msg00007.html https://usn.ubuntu.com/3799-2/ https://usn.ubuntu.com/3799-1/ https://security.netapp.com/advisory/ntap-20181018-0002/	
Pivotal Software					
Spring Security Oauth					
NA	18-10-2018	**6.8**	Spring Security OAuth, versions 2.3 prior to 2.3.4, and 2.2 prior to 2.2.3, and 2.1 prior to 2.1.3, and 2.0 prior to 2.0.16, and older unsupported versions could be susceptible to a privilege escalation under certain conditions. A malicious user or attacker can craft a request to the approval endpoint that can modify the previously saved authorization request and lead to a privilege escalation on the subsequent approval. This scenario can happen if the application is configured to use a custom approval endpoint that declares AuthorizationRequest as a controller method argument. This vulnerability exposes applications that meet all of the following requirements: Act in the role of an Authorization	https://pivotal.io/security/cve-2018-15758	A-Piv-Sprin/19-11-18/11

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			Server (e.g. @EnableAuthorizationServer) and use a custom Approval Endpoint that declares AuthorizationRequest as a controller method argument. This vulnerability does not expose applications that: Act in the role of an Authorization Server and use the default Approval Endpoint, act in the role of a Resource Server only (e.g. @EnableResourceServer), act in the role of a Client only (e.g. @EnableOAuthClient). **CVE-ID:CVE-2018-15758**		
Sem-cms					
Semcms					
CSRF	29-10-2018	**6.8**	A CSRF issue was discovered in SEMCMS 3.4 via the admin/SEMCMS_User.php?Class=add&CF=user URI. **CVE-ID:CVE-2018-18742**	https://github.com/AvaterXXX/SEMCMS/blob/master/CSRF.md	A-Sem-Semcm/19-11-18/12
Wuzhicms					
Wuzhi Cms					
CSRF	29-10-2018	**6.8**	An issue was discovered in WUZHI CMS 4.1.0. There is a CSRF vulnerability that can change the super administrator's password via index.php?m=core&f=panel&v=edit_info. **CVE-ID:CVE-2018-18711**	https://github.com/wuzhicms/wuzhicms/issues/156	A-Wuz-Wuzhi/19-11-18/14
CSRF	29-10-2018	**6.8**	An issue was discovered in WUZHI CMS 4.1.0. There is a CSRF vulnerability that can change the super administrator's username via index.php?m=member&f=index&v=edit&uid=1. **CVE-ID:CVE-2018-18712**	https://github.com/wuzhicms/wuzhicms/issues/156	A-Wuz-Wuzhi/19-11-18/15

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
XSS	05-11-2018	**3.5**	An issue was discovered in WUZHI CMS 4.1.0. There is stored XSS in index.php?m=core&f=index via an ontoggle attribute to details/open/ within a second input field. **CVE-ID:CVE-2018-18938**	https://github.com/wuzhicms/wuzhicms/issues/158	A-Wuz-Wuzhi/19-11-18/16
Wuzhi Cms Project					
Wuzhi Cms					
XSS	05-11-2018	**3.5**	An issue was discovered in WUZHI CMS 4.1.0. There is stored XSS in index.php?m=core&f=index via a seventh input field. **CVE-ID:CVE-2018-18939**	https://github.com/wuzhicms/wuzhicms/issues/159	A-Wuz-Wuzhi/19-11-18/13
Application Operating System (Application,OS)					
Oracle,Redhat					
Enterprise Linux Desktop,Enterprise Linux Server,Enterprise Linux Server Eus,Enterprise Linux Workstation,JDK,JRE					
NA	16-10-2018	**5.1**	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Hotspot). Supported versions that are affected are Java SE: 7u191, 8u182 and 11; Java SE Embedded: 8u181. Difficult to exploit vulnerability allows unauthenticated 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 and while the vulnerability is in Java SE, Java SE Embedded, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE, Java SE Embedded. Note: This	https://access.redhat.com/errata/RHSA-2018:3521 https://access.redhat.com/errata/RHSA-2018:2942 https://access.redhat.com/errata/RHSA-2018:2943 https://usn.ubuntu.com/3824-1/ https://usn.ubuntu.com/3804-1/ https://access.redhat.com/errata/RHSA-2018:3409 https://security.netapp.com/advisory/ntap-20181018-0001/ https://access.redhat.com/errata/R	A-Ora-Enter/19-11-18/21

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g. code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g. code installed by an administrator). CVSS 3.0 Base Score 8.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H). **CVE-ID:CVE-2018-3169**	HSA-2018:3534 https://access.redhat.com/errata/RHSA-2018:3533 https://access.redhat.com/errata/RHSA-2018:3003 https://access.redhat.com/errata/RHSA-2018:3000 https://access.redhat.com/errata/RHSA-2018:3350 https://access.redhat.com/errata/RHSA-2018:3002 https://access.redhat.com/errata/RHSA-2018:3001 https://www.debian.org/security/2018/dsa-4326	
Enterprise Linux Desktop,Enterprise Linux Server,Enterprise Linux Server Eus,Enterprise Linux Workstation,JDK,JRE,Jrockit					
DoS	16-10-2018	**5**	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: Sound). Supported versions that are affected are Java SE: 6u201, 7u191 and 8u182; Java SE Embedded: 8u181; JRockit: R28.3.19. Easily exploitable 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	https://www.debian.org/security/2018/dsa-4326 https://usn.ubuntu.com/3804-1/ https://access.redhat.com/errata/RHSA-2018:3533 https://security.netapp.com/advisory/ntap-20181018-0001/ https://access.redhat.com/errata/RHSA-2018:3534 https://access.redhat.com/errata/RHSA-2018:3350	A-Ora-Enter/19-11-18/17

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			Embedded, JRockit. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g. through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE-ID:CVE-2018-3214**	https://access.redhat.com/errata/RHSA-2018:3409 https://access.redhat.com/errata/RHSA-2018:3003 https://access.redhat.com/errata/RHSA-2018:3007 https://access.redhat.com/errata/RHSA-2018:3008 https://access.redhat.com/errata/RHSA-2018:3002 https://access.redhat.com/errata/RHSA-2018:3001 https://access.redhat.com/errata/RHSA-2018:2943 https://access.redhat.com/errata/RHSA-2018:2942 https://access.redhat.com/errata/RHSA-2018:3000	
DoS	16-10-2018	**6.8**	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: JSSE). Supported versions that are affected are Java SE: 6u201, 7u191, 8u182 and 11; Java SE Embedded: 8u181; JRockit: R28.3.19. Difficult to exploit vulnerability allows unauthenticated attacker with network access via SSL/TLS to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of	https://access.redhat.com/errata/RHSA-2018:3007 https://access.redhat.com/errata/RHSA-2018:2942 https://access.redhat.com/errata/RHSA-2018:3000 https://www.debian.org/security/2018/dsa-4326 https://usn.ubuntu.com/3824-1/ https://usn.ubuntu.com/3804-1/	A-Ora-Enter/19-11-18/18

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			Java SE, Java SE Embedded, JRockit accessible data as well as unauthorized read access to a subset of Java SE, Java SE Embedded, JRockit accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded, JRockit. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g. code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g. through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L). **CVE-ID:CVE-2018-3180**	https://security.netapp.com/advisory/ntap-20181018-0001/ https://access.redhat.com/errata/RHSA-2018:3350 https://access.redhat.com/errata/RHSA-2018:3409 https://access.redhat.com/errata/RHSA-2018:3521 https://access.redhat.com/errata/RHSA-2018:3533 https://access.redhat.com/errata/RHSA-2018:3001 https://access.redhat.com/errata/RHSA-2018:3002 https://access.redhat.com/errata/RHSA-2018:3534 https://access.redhat.com/errata/RHSA-2018:3008 https://access.redhat.com/errata/RHSA-2018:3003 https://access.redhat.com/errata/RHSA-2018:2943	
NA	16-10-2018	**5.1**	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: JNDI). Supported versions that are affected are Java SE: 6u201, 7u191, 8u182 and 11; Java SE Embedded: 8u181; JRockit: R28.3.19. Difficult to exploit vulnerability allows	https://usn.ubuntu.com/3804-1/ https://access.redhat.com/errata/RHSA-2018:3534 https://www.debian.org/security/2018/dsa-4326 https://usn.ubunt	A-Ora-Enter/19-11-18/19

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
			unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, Java SE Embedded, JRockit, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE, Java SE Embedded, JRockit. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g. code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g. through a web service which supplies data to the APIs. CVSS 3.0 Base Score 8.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H). **CVE-ID:CVE-2018-3149**	u.com/3824-1/ https://access.redhat.com/errata/RHSA-2018:3521 https://access.redhat.com/errata/RHSA-2018:3533 https://security.netapp.com/advisory/ntap-20181018-0001/ https://access.redhat.com/errata/RHSA-2018:3000 https://access.redhat.com/errata/RHSA-2018:3409 https://access.redhat.com/errata/RHSA-2018:3008 https://access.redhat.com/errata/RHSA-2018:3002 https://access.redhat.com/errata/RHSA-2018:3003 https://access.redhat.com/errata/RHSA-2018:3007 https://access.redhat.com/errata/RHSA-2018:2943 https://access.redhat.com/errata/RHSA-2018:3350 https://access.redhat.com/errata/RHSA-2018:3001 https://access.redhat.com/errata/RHSA-2018:2942	

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/Patch	NCIIPC ID
NA	16-10-2018	**6.8**	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: Scripting). Supported versions that are affected are Java SE: 8u182 and 11; Java SE Embedded: 8u181; JRockit: R28.3.19. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. While the vulnerability is in Java SE, Java SE Embedded, JRockit, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE, Java SE Embedded, JRockit. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g. code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g. through a web service which supplies data to the APIs. CVSS 3.0 Base Score 9.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H). **CVE-ID:CVE-2018-3183**	https://access.redhat.com/errata/RHSA-2018:3002 https://www.debian.org/security/2018/dsa-4326 https://usn.ubuntu.com/3804-1/ https://access.redhat.com/errata/RHSA-2018:3521 https://access.redhat.com/errata/RHSA-2018:3534 https://security.netapp.com/advisory/ntap-20181018-0001/ https://access.redhat.com/errata/RHSA-2018:3003 https://access.redhat.com/errata/RHSA-2018:3533 https://access.redhat.com/errata/RHSA-2018:2943 https://access.redhat.com/errata/RHSA-2018:2942	A-Ora-Enter/19-11-18/20

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

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