Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Application					
Atlassian					
Jira					
NA	17-01-2018	3.5	The Trello importer in Atlassian Jira before version 7.6.1 allows remote attackers to access the content of internal network resources via a Server Side Request Forgery (SSRF). When running in an environment like Amazon EC2, this flaw maybe used to access to a metadata resource that provides access credentials and other potentially confidential information. **CVE ID : CVE-2017-16865**	https://jira.atlassian.com/browse/JRASERVER-66642	A-ATL-JIRA-010218/1
Banconeon					
Neon					
Gain Information	17-01-2018	4.3	The Neon app 1.6.14 iOS does not verify X.509 certificates from SSL servers, which allows remote attackers to spoof servers and obtain sensitive information via a crafted certificate. **CVE ID : CVE-2018-5258**	NA	A-BAN-NEON-010218/2
Delayed Job Web Project					
Delayed Job Web					
XSS	19-01-2018	4.3	An exploitable cross site scripting (XSS) vulnerability exists in the filter functionality of the delayed_job_web rails gem version 1.4. A specially crafted URL can cause an XSS flaw resulting in an attacker being able to execute arbitrary javascript on the victim's browser. An attacker can phish an authenticated user to trigger this vulnerability. **CVE ID : CVE-2017-12097**	NA	A-DEL-DELAY-010218/3
Download Manager Project					
Download Manager					
XSS	16-01-2018	4.3	The download-manager plugin before 2.9.52 for WordPress has XSS via the id	NA	A-DOW-DOWNL-

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			parameter in a wpdm_generate_password action to wp-admin/admin-ajax.php. **CVE ID : CVE-2017-18032**		010218/4
Ethereum					
Cpp-ethereum					
Bypass	19-01-2018	4.3	An exploitable improper authorization vulnerability exists in admin_peers API of cpp-ethereum's JSON-RPC (commit 4e1015743b95821849d001618a7ce82c7c073768). A JSON request can cause an access to the restricted functionality resulting in authorization bypass. An attacker can send JSON to trigger this vulnerability. **CVE ID : CVE-2017-12114**	NA	A-ETH-CPP-E-010218/5
Exiv2					
Exiv2					
DoS Overflow	18-01-2018	4.3	In Exiv2 0.26, there is a segmentation fault caused by uncontrolled recursion in the Exiv2::Image::printIFDStructure function in the image.cpp file. Remote attackers could leverage this vulnerability to cause a denial of service via a crafted tif file. **CVE ID : CVE-2018-5772**	NA	A-EXI-EXIV2-010218/6
Hancom					
Thinkfree Office Neo					
Execute Code Overflow	17-01-2018	7.5	Hancom NEO versions 9.6.1.5183 and earlier have a buffer Overflow vulnerability that leads remote attackers to execute arbitrary commands when performing the hyperlink Attributes in document. **CVE ID : CVE-2018-5195**	http://help.hancom.com/cve/hoffice/en-US/CVE_en_050_01.htm	A-HAN-THINK-010218/7
IBM					
Rational Engineering Lifecycle Manager					
XSS	16-01-2018	3.5	Cross-site scripting (XSS) vulnerability in IBM Rational Engineering Lifecycle Manager 3.0 before 3.0.1.6 iFix7 Interim Fix 1, 4.0 before 4.0.7 iFix10, 5.0 before 5.0.2 iFix15, and 6.0 before	http://www-01.ibm.com/support/docview.wss?ui	A-IBM-RATIO-010218/8

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	Patch	NCIIPC ID
			6.0.1 iFix4 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors. IBM X-Force ID: 108633. **CVE ID : CVE-2015-7486**	d=swg21983720	
XSS	16-01-2018	3.5	Cross-site scripting (XSS) vulnerability in IBM Rational Engineering Lifecycle Manager 3.0 before 3.0.1.6 iFix7 Interim Fix 1, 4.0 before 4.0.7 iFix10, 5.0 before 5.0.2 iFix15, and 6.0 before 6.0.1 iFix4 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors. IBM X-Force ID: 108626. **CVE ID : CVE-2015-7485**	http://www-01.ibm.com/support/docview.wss?uid=swg21983720	A-IBM-RATIO-010218/9
XSS	16-01-2018	3.5	Cross-site scripting (XSS) vulnerability in Jazz Foundation in IBM Rational Engineering Lifecycle Manager 3.0 before 3.0.1.6 iFix7 Interim Fix 1, 4.0 before 4.0.7 iFix10, 5.0 before 5.0.2 iFix15, and 6.0 before 6.0.1 iFix4 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors. IBM X-Force ID: 108501. **CVE ID : CVE-2015-7474**	http://www-01.ibm.com/support/docview.wss?uid=swg21983720	A-IBM-RATIO-010218/10
Gain Information	16-01-2018	4	IBM Rational Engineering Lifecycle Manager 3.0 before 3.0.1.6 iFix7 Interim Fix 1 and 4.0 before 4.0.7 iFix10 allow remote authenticated users with access to lifecycle projects to obtain sensitive information by sending a crafted URL to the Lifecycle Query Engine. IBM X-Force ID: 108619. **CVE ID : CVE-2015-7484**	http://www-01.ibm.com/support/docview.wss?uid=swg21983720	A-IBM-RATIO-010218/11
Jquery					
Jquery					
XSS	16-01-2018	4.3	jQuery 1.4.2 allows remote attackers to conduct cross-site scripting (XSS) attacks via vectors related to use of the text method inside after. **CVE ID : CVE-2014-6071**	https://bugzilla.redhat.com/show_bug.cgi?id=1136683	A-JQU-JQUER-010218/12
XSS	18-01-2018	4.3	jQuery before 3.0.0 is vulnerable to Cross-site Scripting (XSS) attacks when a cross-domain Ajax request is performed without the dataType	NA	A-JQU-JQUER-010218/13

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			option, causing text/javascript responses to be executed. **CVE ID : CVE-2015-9251**		
XSS	18-01-2018	4.3	jQuery before 1.9.0 is vulnerable to Cross-site Scripting (XSS) attacks. The jQuery(strInput) function does not differentiate selectors from HTML in a reliable fashion. In vulnerable versions, jQuery determined whether the input was HTML by looking for the '<' character anywhere in the string, giving attackers more flexibility when attempting to construct a malicious payload. In fixed versions, jQuery only deems the input to be HTML if it explicitly starts with the '<' character, limiting exploitability only to attackers who can control the beginning of a string, which is far less common. **CVE ID : CVE-2012-6708**	NA	A-JQU-JQUER-010218/14
DoS	18-01-2018	5	jQuery 3.0.0-rc.1 is vulnerable to Denial of Service (DoS) due to removing a logic that lowercased attribute names. Any attribute getter using a mixed-cased name for boolean attributes goes into an infinite recursion, exceeding the stack call limit. **CVE ID : CVE-2016-10707**	NA	A-JQU-JQUER-010218/15
Libav					
Libav					
DoS Overflow	18-01-2018	6.8	In Libav through 12.2, there is an invalid memcpy in the av_packet_ref function of libavcodec/avpacket.c. Remote attackers could leverage this vulnerability to cause a denial of service (segmentation fault) via a crafted avi file. **CVE ID : CVE-2018-5766**	NA	A-LIB-LIBAV-010218/16
Libtiff					
Libtiff					
DoS	19-01-2018	4.3	In LibTIFF 4.0.9, there is an uncontrolled resource consumption in the TIFFSetDirectory function of tif_dir.c. Remote attackers could	http://bugzilla.maptools.org/show_bug.cgi?id=27	A-LIB-LIBTI-010218/17

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	Patch	NCIIPC ID
			leverage this vulnerability to cause a denial of service via a crafted tif file. This occurs because the declared number of directory entries is not validated against the actual number of directory entries. **CVE ID : CVE-2018-5784**	72	
Livezilla					
Livezilla					
XSS	18-01-2018	4.3	Cross-site scripting (XSS) vulnerability in knowledgebase.php in LiveZilla before 7.0.8.9 allows remote attackers to inject arbitrary web script or HTML via the search-for parameter. **CVE ID : CVE-2017-15869**	https://www.livezilla.net/changelog/en/	A-LIV-LIVEZ-010218/18
Lrzip Project					
Lrzip					
DoS	17-01-2018	4.3	In Long Range Zip (aka lrzip) 0.631, there is a use-after-free in the ucompthread function (stream.c). Remote attackers could leverage this vulnerability to cause a denial of service via a crafted lrz file. **CVE ID : CVE-2018-5747**	https://github.com/ckolivas/lrzip/issues/90	A-LRZ-LRZIP-010218/19
MIT					
Kerberos					
DoS	16-01-2018	4	An issue was discovered in MIT Kerberos 5 (aka krb5) through 1.16. The pre-defined function "strlen" is getting a "NULL" string as a parameter value in plugins/kdb/ldap/libkdb_ldap/ldap_principal2.c in the Key Distribution Center (KDC), which allows remote authenticated users to cause a denial of service (NULL pointer dereference) via a modified kadmin client. **CVE ID : CVE-2018-5710**	https://github.com/poojamnit/Kerberos-V5-1.16-Vulnerabilities/tree/master/Denial%20Of%20Service%28DoS%29	A-MIT-KERBE-010218/20
NA	16-01-2018	5	An issue was discovered in MIT Kerberos 5 (aka krb5) through 1.16. There is a variable "dbentry->n_key_data" in kadmin/dbutil/dump.c	https://github.com/poojamnit/Kerberos-V5-1.16-	A-MIT-KERBE-010218/21

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	Patch	NCIIPC ID
			that can store 16-bit data but unknowingly the developer has assigned a "u4" variable to it, which is for 32-bit data. An attacker can use this vulnerability to affect other artifacts of the database as we know that a Kerberos database dump file contains trusted data. **CVE ID : CVE-2018-5709**	Vulnerabilities/tree/master/Integer%20Overflow	
Octopus					
Octopus Deploy					
NA	16-01-2018	6.5	An issue was discovered in Octopus Deploy before 4.1.9. Any user with user editing permissions can modify teams to give themselves Administer System permissions even if they didn't have them, as demonstrated by use of the RoleEdit or TeamEdit permission. **CVE ID : CVE-2018-5706**	https://github.com/OctopusDeploy/Issues/issues/4167	A-OCT-OCTOP-010218/22
Openjpeg					
Openjpeg					
DoS Overflow	16-01-2018	4.3	In OpenJPEG 2.3.0, there is an integer overflow vulnerability in the opj_t1_encode_cblks function (openjp2/t1.c). Remote attackers could leverage this vulnerability to cause a denial of service via a crafted bmp file. **CVE ID : CVE-2018-5727**	https://github.com/uclouvain/openjpeg/issues/1053	A-OPE-OPENJ-010218/23
DoS Overflow	19-01-2018	4.3	In OpenJPEG 2.3.0, there is an integer overflow caused by an out-of-bounds left shift in the opj_j2k_setup_encoder function (openjp2/j2k.c). Remote attackers could leverage this vulnerability to cause a denial of service via a crafted bmp file. **CVE ID : CVE-2018-5785**	https://github.com/uclouvain/openjpeg/issues/1057	A-OPE-OPENJ-010218/24
Oracle					
Access Manager					
Gain Information	17-01-2018	4.3	Vulnerability in the Oracle Access Manager component of Oracle Fusion Middleware (subcomponent: Web Server Plugin). The supported version	http://www.oracle.com/technetwork/security-	A-ORA-ACCES-010218/25

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	Patch	NCIIPC ID
			that is affected is 11.1.2.3.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Oracle Access Manager. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Access Manager accessible data. CVSS 3.0 Base Score 5.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2017-10262**	advisory/cpujan2018-3236628.html	
Agile Product Lifecycle Management Framework					
NA	17-01-2018	5.8	Vulnerability in the Oracle Agile PLM component of Oracle Supply Chain Products Suite (subcomponent: Security). Supported versions that are affected are 9.3.5 and 9.3.6. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Agile PLM. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Agile PLM, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Agile PLM accessible data as well as unauthorized read access to a subset of Oracle Agile PLM 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-2018-2609**	http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html	A-ORA-AGILE-010218/26
Application Express					
NA	17-01-2018	5.8	Vulnerability in the Application Express component of Oracle Database Server.	http://www.oracle.com/t	A-ORA-APPLI-

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			The supported version that is affected is Prior to 5.1.4.00.08. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Application Express. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Application Express, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Application Express accessible data as well as unauthorized read access to a subset of Application Express 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-2018-2699**	echnetwork/security-advisory/cpujan2018-3236628.html	010218/27
Banking Corporate Lending					
Gain Information	17-01-2018	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 and 12.4.0. 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 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-2018-2709**	http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html	A-ORA-BANKI-010218/28
NA	17-01-2018	6.5	Vulnerability in the Oracle Banking	http://www.	A-ORA-

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Corporate Lending component of Oracle Financial Services Applications (subcomponent: Core module). Supported versions that are affected are 12.3.0 and 12.4.0. 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 takeover of Oracle Banking Corporate Lending. CVSS 3.0 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H). **CVE ID : CVE-2018-2706**	oracle.com/technetwork/security-advisory/cpujan2018-3236628.html	BANKI-010218/29
NA	17-01-2018	7.5	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 and 12.4.0. 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 and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Banking Corporate Lending. CVSS 3.0 Base Score 8.1 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:H). **CVE ID : CVE-2018-2707**	http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html	A-ORA-BANKI-010218/30
Banking Payments					
Gain Information	17-01-2018	3.5	Vulnerability in the Oracle Banking Payments component of Oracle	http://www.oracle.com/t	A-ORA-BANKI-

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	Patch	NCIIPC ID
			Financial Services Applications (subcomponent: Payments Core). Supported versions that are affected are 12.3.0 and 12.4.0. 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 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-2018-2708**	echnetwork/ security-advisory/cp ujan2018-3236628.ht ml	010218/31
NA	17-01-2018	6.5	Vulnerability in the Oracle Banking Payments component of Oracle Financial Services Applications (subcomponent: Payments Core). Supported versions that are affected are 12.3.0 and 12.4.0. 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 takeover of Oracle Banking Payments. CVSS 3.0 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C :H/I:H/A:H). **CVE ID : CVE-2018-2705**	http://www. oracle.com/t echnetwork/ security-advisory/cp ujan2018-3236628.ht ml	A-ORA-BANKI-010218/32
NA	17-01-2018	7.5	Vulnerability in the Oracle Banking Payments component of Oracle Financial Services Applications (subcomponent: Payments Core). Supported versions that are affected are 12.3.0 and 12.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Banking	http://www. oracle.com/t echnetwork/ security-advisory/cp ujan2018-3236628.ht ml	A-ORA-BANKI-010218/33

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	Patch	NCIIPC ID
			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 and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Banking Payments. CVSS 3.0 Base Score 8.1 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:H). **CVE ID : CVE-2018-2704**		
Business Intelligence					
Gain Information	17-01-2018	4	Vulnerability in the Oracle Business Intelligence Enterprise Edition component of Oracle Fusion Middleware (subcomponent: BI Platform Security). Supported versions that are affected are 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 Business Intelligence Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Business Intelligence Enterprise Edition 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-2018-2715**	http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html	A-ORA-BUSIN-010218/34
NA	17-01-2018	6.4	Vulnerability in the Oracle Business Intelligence Enterprise Edition component of Oracle Fusion Middleware (subcomponent: Analytics Web Dashboards). The supported version that is affected is 12.2.1.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network	http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html	A-ORA-BUSIN-010218/35

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Business Intelligence Enterprise Edition, 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 Business Intelligence Enterprise Edition accessible data as well as unauthorized update, insert or delete access to some of Oracle Business Intelligence Enterprise Edition 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-2017-10068**		
Database Server					
NA	17-01-2018	5.1	Vulnerability in the Java VM component of Oracle Database Server. Supported versions that are affected are 11.2.0.4, 12.1.0.2 and 12.2.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java VM. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java VM, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java VM. 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-2018-2680**	http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html	A-ORA-DATAB-010218/36
NA	17-01-2018	6.5	Vulnerability in the Core RDBMS	http://www.	A-ORA-

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	Patch	NCIIPC ID
			component of Oracle Database Server. Supported versions that are affected are 12.1.0.2 and 12.2.0.1. Easily exploitable vulnerability allows high privileged attacker having Create Session, Execute Catalog Role privilege with network access via Oracle Net 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 takeover of Core RDBMS. CVSS 3.0 Base Score 9.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H). **CVE ID : CVE-2017-10282**	oracle.com/technetwork/security-advisory/cpujan2018-3236628.html	DATAB-010218/37
E-business Suite					
Gain Information	17-01-2018	4	Vulnerability in the Oracle User Management component of Oracle E-Business Suite (subcomponent: Registration Process). 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 high privileged attacker with network access via HTTP to compromise Oracle User Management. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle User Management accessible data. CVSS 3.0 Base Score 4.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2018-2684**	http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html	A-ORA-E-BUS-010218/38
NA	17-01-2018	5.8	Vulnerability in the Oracle Application Object Library component of Oracle E-Business Suite (subcomponent: Login). Supported versions that are affected are 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6	http://www.oracle.com/technetwork/security-advisory/cp	A-ORA-E-BUS-010218/39

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and 12.2.7. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Application Object Library. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Application Object Library accessible data as well as unauthorized read access to a subset of Oracle Application Object Library accessible data. CVSS 3.0 Base Score 4.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N). **CVE ID : CVE-2018-2635**	ujan2018-3236628.html	
NA	17-01-2018	6.4	Vulnerability in the Oracle General Ledger component of Oracle E-Business Suite (subcomponent: Data Manager Server). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6 and 12.2.7. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle General Ledger. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle General Ledger accessible data as well as unauthorized access to critical data or complete access to all Oracle General Ledger accessible data. CVSS 3.0 Base Score 9.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N). **CVE ID : CVE-2018-2656**	http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html	A-ORA-E-BUS-010218/40
Financial Services Analytical Applications Infrastructure					
NA	17-01-2018	5.8	Vulnerability in the Oracle Financial Services Analytical Applications Infrastructure component of Oracle	http://www.oracle.com/technetwork/	A-ORA-FINAN-010218/41

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Financial Services Applications (subcomponent: Core). Supported versions that are affected are 7.3.5.x and 8.0.x. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Financial Services Analytical Applications Infrastructure. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Financial Services Analytical Applications Infrastructure, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Financial Services Analytical Applications Infrastructure accessible data as well as unauthorized read access to a subset of Oracle Financial Services Analytical Applications Infrastructure 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-2018-2661**	security-advisory/cpujan2018-3236628.html	
DoS	17-01-2018	6.5	Vulnerability in the Oracle Financial Services Analytical Applications Infrastructure component of Oracle Financial Services Applications (subcomponent: Core). Supported versions that are affected are 7.3.5.x and 8.0.x. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Financial Services Analytical Applications Infrastructure. While the vulnerability is in Oracle Financial Services Analytical Applications Infrastructure, attacks	http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html	A-ORA-FINAN-010218/42

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	Patch	NCIIPC ID
			may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Financial Services Analytical Applications Infrastructure accessible data as well as unauthorized read access to a subset of Oracle Financial Services Analytical Applications Infrastructure accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Financial Services Analytical Applications Infrastructure. CVSS 3.0 Base Score 7.4 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:L). **CVE ID : CVE-2018-2660**		
Financial Services Analytical Applications Reconciliation Framework					
NA	17-01-2018	5.8	Vulnerability in the Oracle Financial Services Analytical Applications Reconciliation Framework component of Oracle Financial Services Applications (subcomponent: User Interface). The supported version that is affected is 8.0.x. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Financial Services Analytical Applications Reconciliation Framework. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Financial Services Analytical Applications Reconciliation Framework, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Financial	http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html	A-ORA-FINAN-010218/43

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Services Analytical Applications Reconciliation Framework accessible data as well as unauthorized read access to a subset of Oracle Financial Services Analytical Applications Reconciliation Framework 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-2018-2732**		
Financial Services Asset Liability Management					
NA	17-01-2018	5.5	Vulnerability in the Oracle Financial Services Asset Liability Management component of Oracle Financial Services Applications (subcomponent: User Interface). Supported versions that are affected are 6.1.x and 8.0.x. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Financial Services Asset Liability Management. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Financial Services Asset Liability Management accessible data as well as unauthorized access to critical data or complete access to all Oracle Financial Services Asset Liability 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-2018-2723**	http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html	A-ORA-FINAN-010218/44
NA	17-01-2018	5.8	Vulnerability in the Oracle Financial Services Asset Liability Management component of Oracle Financial Services Applications (subcomponent: User Interface). Supported versions that are	http://www.oracle.com/technetwork/security-advisory/cp	A-ORA-FINAN-010218/45

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected are 6.1.x and 8.0.x. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Financial Services Asset Liability Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Financial Services Asset Liability 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 Financial Services Asset Liability Management accessible data as well as unauthorized read access to a subset of Oracle Financial Services Asset Liability 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-2018-2692**	ujan2018-3236628.html	
Financial Services Balance Sheet Planning					
NA	17-01-2018	5.5	Vulnerability in the Oracle Financial Services Balance Sheet Planning component of Oracle Financial Services Applications (subcomponent: User Interface). The supported version that is affected is 8.0.x. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Financial Services Balance Sheet Planning. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Financial Services Balance Sheet Planning accessible data as well as unauthorized access to critical data or complete	http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html	A-ORA-FINAN-010218/46

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	Patch	NCIIPC ID
			access to all Oracle Financial Services Balance Sheet Planning 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-2018-2592**		
NA	17-01-2018	5.8	Vulnerability in the Oracle Financial Services Balance Sheet Planning component of Oracle Financial Services Applications (subcomponent: User Interface). The supported version that is affected is 8.0.x. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Financial Services Balance Sheet Planning. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Financial Services Balance Sheet Planning, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Financial Services Balance Sheet Planning accessible data as well as unauthorized read access to a subset of Oracle Financial Services Balance Sheet Planning 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-2018-2626**	http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html	A-ORA-FINAN-010218/47
Financial Services Funds Transfer Pricing					
NA	17-01-2018	5.8	Vulnerability in the Oracle Financial Services Funds Transfer Pricing component of Oracle Financial Services Applications (subcomponent: User Interface). Supported versions that are affected are 6.1.x and 8.0.x. Easily	http://www.oracle.com/technetwork/security-advisory/cpujan2018-	A-ORA-FINAN-010218/48

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Financial Services Funds Transfer Pricing. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Financial Services Funds Transfer Pricing accessible data as well as unauthorized access to critical data or complete access to all Oracle Financial Services Funds Transfer Pricing 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-2018-2729**	3236628.html	
NA	17-01-2018	5.8	Vulnerability in the Oracle Financial Services Funds Transfer Pricing component of Oracle Financial Services Applications (subcomponent: User Interface). Supported versions that are affected are 6.1.x and 8.0.x. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Financial Services Funds Transfer Pricing. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Financial Services Funds Transfer Pricing, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Financial Services Funds Transfer Pricing accessible data as well as unauthorized read access to a subset of Oracle Financial Services Funds Transfer Pricing accessible data. CVSS	http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html	A-ORA-FINAN-010218/49

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	Patch	NCIIPC ID
			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-2018-2728**		
Financial Services Hedge Management And Ifrs Valuations					
NA	17-01-2018	5.5	Vulnerability in the Oracle Financial Services Hedge Management and IFRS Valuations component of Oracle Financial Services Applications (subcomponent: User Interface). The supported version that is affected is 8.0.x. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Financial Services Hedge Management and IFRS Valuations. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Financial Services Hedge Management and IFRS Valuations accessible data as well as unauthorized access to critical data or complete access to all Oracle Financial Services Hedge Management and IFRS Valuations 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-2018-2725**	http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html	A-ORA-FINAN-010218/50
NA	17-01-2018	5.8	Vulnerability in the Oracle Financial Services Hedge Management and IFRS Valuations component of Oracle Financial Services Applications (subcomponent: User Interface). The supported version that is affected is 8.0.x. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Financial Services Hedge Management and IFRS	http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html	A-ORA-FINAN-010218/51

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Valuations. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Financial Services Hedge Management and IFRS Valuations, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Financial Services Hedge Management and IFRS Valuations accessible data as well as unauthorized read access to a subset of Oracle Financial Services Hedge Management and IFRS Valuations 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-2018-2719**		
Financial Services Liquidity Risk Management					
NA	17-01-2018	5.5	Vulnerability in the Oracle Financial Services Liquidity Risk Management component of Oracle Financial Services Applications (subcomponent: User Interface). The supported version that is affected is 8.0.x. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Financial Services Liquidity Risk Management. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Financial Services Liquidity Risk Management accessible data as well as unauthorized access to critical data or complete access to all Oracle Financial Services Liquidity Risk Management accessible data. CVSS 3.0 Base Score 8.1 (Confidentiality and Integrity impacts).	http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html	A-ORA-FINAN-010218/52

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N). **CVE ID : CVE-2018-2720**		
NA	17-01-2018	5.8	Vulnerability in the Oracle Financial Services Liquidity Risk Management component of Oracle Financial Services Applications (subcomponent: User Interface). The supported version that is affected is 8.0.x. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Financial Services Liquidity Risk Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Financial Services Liquidity Risk 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 Financial Services Liquidity Risk Management accessible data as well as unauthorized read access to a subset of Oracle Financial Services Liquidity Risk 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-2018-2682**	http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html	A-ORA-FINAN-010218/53
Financial Services Loan Loss Forecasting And Provisioning					
NA	17-01-2018	5.5	Vulnerability in the Oracle Financial Services Loan Loss Forecasting and Provisioning component of Oracle Financial Services Applications (subcomponent: User Interface). The supported version that is affected is 8.0.x. Easily exploitable vulnerability allows low privileged attacker with	http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html	A-ORA-FINAN-010218/54

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	Patch	NCIIPC ID
			network access via HTTP to compromise Oracle Financial Services Loan Loss Forecasting and Provisioning. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Financial Services Loan Loss Forecasting and Provisioning accessible data as well as unauthorized access to critical data or complete access to all Oracle Financial Services Loan Loss Forecasting and Provisioning 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-2018-2724**		
NA	17-01-2018	5.8	Vulnerability in the Oracle Financial Services Loan Loss Forecasting and Provisioning component of Oracle Financial Services Applications (subcomponent: User Interface). The supported version that is affected is 8.0.x. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Financial Services Loan Loss Forecasting and Provisioning. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Financial Services Loan Loss Forecasting and Provisioning, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Financial Services Loan Loss Forecasting and Provisioning accessible data as well as unauthorized read access to a subset of	http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html	A-ORA-FINAN-010218/55

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	Patch	NCIIPC ID
			Oracle Financial Services Loan Loss Forecasting and Provisioning 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-2018-2712**		
Financial Services Market Risk					
NA	17-01-2018	5.8	Vulnerability in the Oracle Financial Services Market Risk component of Oracle Financial Services Applications (subcomponent: User Interface). The supported version that is affected is 8.0.x. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Financial Services Market Risk. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Financial Services Market Risk, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Financial Services Market Risk accessible data as well as unauthorized read access to a subset of Oracle Financial Services Market Risk 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-2018-2714**	http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html	A-ORA-FINAN-010218/56
Financial Services Market Risk Measurement And Management					
NA	17-01-2018	5.5	Vulnerability in the Oracle Financial Services Market Risk Measurement and Management component of Oracle Financial Services Applications (subcomponent: User Interface). The	http://www.oracle.com/technetwork/security-advisory/cp	A-ORA-FINAN-010218/57

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			supported version that is affected is 8.0.5. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Financial Services Market Risk Measurement and Management. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Financial Services Market Risk Measurement and Management accessible data as well as unauthorized access to critical data or complete access to all Oracle Financial Services Market Risk Measurement and 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-2018-2727**	ujan2018-3236628.html	
NA	17-01-2018	5.8	Vulnerability in the Oracle Financial Services Market Risk Measurement and Management component of Oracle Financial Services Applications (subcomponent: User Interface). The supported version that is affected is 8.0.5. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Financial Services Market Risk Measurement and Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Financial Services Market Risk Measurement and 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 Financial	http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html	A-ORA-FINAN-010218/58

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	Patch	NCIIPC ID
			Services Market Risk Measurement and Management accessible data as well as unauthorized read access to a subset of Oracle Financial Services Market Risk Measurement and 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-2018-2716**		
Financial Services Price Creation And Discovery					
NA	17-01-2018	5.5	Vulnerability in the Oracle Financial Services Price Creation and Discovery component of Oracle Financial Services Applications (subcomponent: User Interface). The supported version that is affected is 8.0.5. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Financial Services Price Creation and Discovery. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Financial Services Price Creation and Discovery accessible data as well as unauthorized access to critical data or complete access to all Oracle Financial Services Price Creation and Discovery 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-2018-2721**	http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html	A-ORA-FINAN-010218/59
NA	17-01-2018	5.8	Vulnerability in the Oracle Financial Services Price Creation and Discovery component of Oracle Financial Services Applications (subcomponent: User Interface). The supported version that is affected is 8.0.5. Easily exploitable	http://www.oracle.com/technetwork/security-advisory/cpujan2018-	A-ORA-FINAN-010218/60

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Financial Services Price Creation and Discovery. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Financial Services Price Creation and Discovery, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Financial Services Price Creation and Discovery accessible data as well as unauthorized read access to a subset of Oracle Financial Services Price Creation and Discovery 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-2018-2722**	3236628.html	
Financial Services Profitability Management					
NA	17-01-2018	5.5	Vulnerability in the Oracle Financial Services Profitability Management component of Oracle Financial Services Applications (subcomponent: User Interface). Supported versions that are affected are 6.1.x and 8.0.x. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Financial Services Profitability Management. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Financial Services Profitability Management accessible data as well as unauthorized access to critical data or complete access to all Oracle Financial Services Profitability Management	http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html	A-ORA-FINAN-010218/61

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2018-2679**		
NA	17-01-2018	5.8	Vulnerability in the Oracle Financial Services Profitability Management component of Oracle Financial Services Applications (subcomponent: User Interface). Supported versions that are affected are 6.1.x and 8.0.x. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Financial Services Profitability Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Financial Services Profitability 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 Financial Services Profitability Management accessible data as well as unauthorized read access to a subset of Oracle Financial Services Profitability 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-2018-2670**	http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html	A-ORA-FINAN-010218/62
Flexcube Direct Banking					
NA	17-01-2018	5.8	Vulnerability in the Oracle FLEXCUBE Direct Banking component of Oracle Financial Services Applications (subcomponent: Logoff). Supported versions that are affected are 12.0.2 and 12.0.3. Easily exploitable vulnerability	http://www.oracle.com/technetwork/security-advisory/cpujan2018-	A-ORA-FLEXC-010218/63

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	Patch	NCIIPC ID
			allows unauthenticated attacker with network access via HTTP to compromise Oracle FLEXCUBE Direct Banking. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle FLEXCUBE Direct 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 Direct Banking accessible data as well as unauthorized read access to a subset of Oracle FLEXCUBE Direct Banking accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2018-2674**	3236628.html	
Flexcube Universal Banking					
Gain Information	17-01-2018	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 and 12.4.0. 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-2018-2614**	http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html	A-ORA-FLEXC-010218/64

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
NA	17-01-2018	5.5	Vulnerability in the Oracle FLEXCUBE Universal Banking component of Oracle Financial Services Applications (subcomponent: Security Management System). Supported versions that are affected are 11.5.0, 11.6.0 and 11.7.0. 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: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N). **CVE ID : CVE-2018-2630**	http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html	A-ORA-FLEXC-010218/65
NA	17-01-2018	6.4	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 and 12.4.0. 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 creation, deletion or modification access to critical data or all Oracle FLEXCUBE Universal Banking accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle FLEXCUBE Universal Banking. CVSS 3.0 Base Score 8.1	http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html	A-ORA-FLEXC-010218/66

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	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:H/A:H). **CVE ID : CVE-2018-2649**		
NA	17-01-2018	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 and 12.4.0. 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 takeover of Oracle FLEXCUBE Universal Banking. CVSS 3.0 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H). **CVE ID : CVE-2018-2648**	http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html	A-ORA-FLEXC-010218/67
Hospitality Cruise Dining Room Management					
NA	17-01-2018	5.8	Vulnerability in the Oracle Hospitality Cruise Dining Room Management component of Oracle Hospitality Applications (subcomponent: SilverWhere). The supported version that is affected is 8.0.78. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hospitality Cruise Dining Room Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Hospitality Cruise Dining Room Management, attacks may significantly impact additional products. Successful attacks	http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html	A-ORA-HOSPI-010218/68

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hospitality Cruise Dining Room Management accessible data as well as unauthorized update, insert or delete access to some of Oracle Hospitality Cruise Dining Room 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-2018-2597**		
Hospitality Cruise Fleet Management					
NA	17-01-2018	4.9	Vulnerability in the Oracle Hospitality Cruise Fleet Management component of Oracle Hospitality Applications (subcomponent: Emergency Response System). The supported version that is affected is 9.0.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hospitality Cruise Fleet Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Hospitality Cruise Fleet 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 Hospitality Cruise Fleet Management accessible data as well as unauthorized update, insert or delete access to some of Oracle Hospitality Cruise Fleet Management accessible data. CVSS 3.0 Base Score 7.6 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:L/A:N).	http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html	A-ORA-HOSPI-010218/69

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	Patch	NCIIPC ID
			CVE ID : CVE-2018-2701		
Gain Information	17-01-2018	5	Vulnerability in the Oracle Hospitality Cruise Fleet Management component of Oracle Hospitality Applications (subcomponent: Emergency Response System). The supported version that is affected is 9.0.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hospitality Cruise Fleet Management. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hospitality Cruise Fleet Management 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-2018-2700**	http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html	A-ORA-HOSPI-010218/70
NA	17-01-2018	6.4	Vulnerability in the Oracle Hospitality Cruise Fleet Management component of Oracle Hospitality Applications (subcomponent: Emergency Response System). The supported version that is affected is 9.0.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hospitality Cruise Fleet Management. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hospitality Cruise Fleet Management accessible data as well as unauthorized access to critical data or complete access to all Oracle Hospitality Cruise Fleet Management accessible data. CVSS 3.0 Base Score 9.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N).	http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html	A-ORA-HOSPI-010218/71

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	Patch	NCIIPC ID
			CVE ID : CVE-2018-2697		
Hospitality Cruise Shipboard Property Management System					
NA	17-01-2018	6.4	Vulnerability in the Oracle Hospitality Cruise Shipboard Property Management System component of Oracle Hospitality Applications (subcomponent: Mobile Gangway and Mustering). The supported version that is affected is 7.3.874. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hospitality Cruise Shipboard Property Management System. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hospitality Cruise Shipboard Property Management System accessible data as well as unauthorized update, insert or delete access to some of Oracle Hospitality Cruise Shipboard Property Management System accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N). **CVE ID : CVE-2018-2621**	http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html	A-ORA-HOSPI-010218/72
Hospitality Guest Access					
NA	17-01-2018	4	Vulnerability in the Oracle Hospitality Guest Access component of Oracle Hospitality Applications (subcomponent: Base). The supported version that is affected is 4.2.1. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Hospitality Guest Access. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Hospitality Guest Access. CVSS 3.0 Base Score 4.9	http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html	A-ORA-HOSPI-010218/73

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(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-2018-2607**		
Gain Information	17-01-2018	5	Vulnerability in the Oracle Hospitality Guest Access component of Oracle Hospitality Applications (subcomponent: Base). The supported version that is affected is 4.2.1. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hospitality Guest Access. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hospitality Guest Access 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-2018-2604**	http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html	A-ORA-HOSPI-010218/74
Hospitality Labor Management					
NA	17-01-2018	5.5	Vulnerability in the Oracle Hospitality Labor Management component of Oracle Hospitality Applications (subcomponent: Webservice Endpoint). Supported versions that are affected are 8.5.1 and 9.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hospitality Labor Management. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hospitality Labor Management accessible data as well as unauthorized access to critical data or complete access to all Oracle Hospitality Labor Management accessible data. CVSS 3.0 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector:	http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html	A-ORA-HOSPI-010218/75

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N). **CVE ID : CVE-2018-2666**		
Hospitality Reporting And Analytics					
NA	17-01-2018	5.5	Vulnerability in the Oracle Hospitality Reporting and Analytics component of Oracle Hospitality Applications (subcomponent: Report). Supported versions that are affected are 8.5.1 and 9.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hospitality Reporting and Analytics. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hospitality Reporting and Analytics accessible data as well as unauthorized read access to a subset of Oracle Hospitality Reporting and Analytics accessible data. CVSS 3.0 Base Score 7.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:H/A:N). **CVE ID : CVE-2018-2650**	http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html	A-ORA-HOSPI-010218/76
NA	17-01-2018	5.8	Vulnerability in the Oracle Hospitality Reporting and Analytics component of Oracle Hospitality Applications (subcomponent: Report). Supported versions that are affected are 8.5.1 and 9.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hospitality Reporting and Analytics. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Hospitality Reporting and Analytics, attacks may significantly impact additional products. Successful attacks	http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html	A-ORA-HOSPI-010218/77

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Hospitality Reporting and Analytics accessible data as well as unauthorized read access to a subset of Oracle Hospitality Reporting and Analytics 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-2018-2669**		
Hospitality Simphony					
Gain Information	17-01-2018	4	Vulnerability in the Oracle Hospitality Simphony component of Oracle Hospitality Applications (subcomponent: Security). The supported version that is affected is 2.7. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hospitality Simphony. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hospitality Simphony 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-2018-2619**	http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html	A-ORA-HOSPI-010218/78
Gain Information	17-01-2018	4.3	Vulnerability in the Oracle Hospitality Simphony component of Oracle Hospitality Applications (subcomponent: POS). Supported versions that are affected are 2.7, 2.8 and 2.9. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hospitality Simphony. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete	http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html	A-ORA-HOSPI-010218/79

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			access to all Oracle Hospitality Simphony accessible data. CVSS 3.0 Base Score 5.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/ C:H/I:N/A:N). **CVE ID : CVE-2018-2673**		
NA	17-01-2018	5	Vulnerability in the Oracle Hospitality Simphony component of Oracle Hospitality Applications (subcomponent: POS). Supported versions that are affected are 2.7, 2.8 and 2.9. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hospitality Simphony. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Hospitality Simphony. CVSS 3.0 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/ C:N/I:N/A:H). **CVE ID : CVE-2018-2683**	http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html	A-ORA-HOSPI-010218/80
Gain Information	17-01-2018	5	Vulnerability in the Oracle Hospitality Simphony component of Oracle Hospitality Applications (subcomponent: POS). Supported versions that are affected are 2.7, 2.8 and 2.9. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hospitality Simphony. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hospitality Simphony 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/	http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html	A-ORA-HOSPI-010218/81

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			C:H/I:N/A:N). **CVE ID : CVE-2018-2672**		
Gain Information	17-01-2018	5	Vulnerability in the Oracle Hospitality Simphony component of Oracle Hospitality Applications (subcomponent: Security). The supported version that is affected is 2.7. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hospitality Simphony. While the vulnerability is in Oracle Hospitality Simphony, 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 Hospitality Simphony 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-2018-2608**	http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html	A-ORA-HOSPI-010218/82
Gain Information	17-01-2018	5	Vulnerability in the Oracle Hospitality Simphony component of Oracle Hospitality Applications (subcomponent: Enterprise Server). Supported versions that are affected are 2.7, 2.8 and 2.9. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hospitality Simphony. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hospitality Simphony 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-2018-2589**	http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html	A-ORA-HOSPI-010218/83
NA	17-01-2018	6.8	Vulnerability in the Oracle Hospitality	http://www.	A-ORA-

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Simphony component of Oracle Hospitality Applications (subcomponent: Security). Supported versions that are affected are 2.7, 2.8 and 2.9. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hospitality Simphony. Successful attacks of this vulnerability can result in takeover of Oracle Hospitality Simphony. CVSS 3.0 Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H). **CVE ID : CVE-2018-2636**	oracle.com/technetwork/security-advisory/cpujan2018-3236628.html	HOSPI-010218/84
Http Server					
DoS	17-01-2018	5	Vulnerability in the Oracle HTTP Server component of Oracle Fusion Middleware (subcomponent: Web Listener). 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 unauthenticated attacker with network access via HTTP to compromise Oracle HTTP Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle HTTP Server. 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-2018-2561**	http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html	A-ORA-HTTP - 010218/85
Hyperion Bi+					
DoS	17-01-2018	6	Vulnerability in the Hyperion BI+ component of Oracle Hyperion (subcomponent: Foundation UI & Servlets). The supported version that is affected is 11.1.2.4. Easily exploitable vulnerability allows high privileged	http://www.oracle.com/technetwork/security-advisory/cpujan2018-	A-ORA-HYPER-010218/86

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker with network access via HTTP to compromise Hyperion BI+. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Hyperion BI+ accessible data as well as unauthorized read access to a subset of Hyperion BI+ accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Hyperion BI+. CVSS 3.0 Base Score 4.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/ C:L/I:L/A:L). **CVE ID : CVE-2018-2595**	3236628.html	
DoS	17-01-2018	6	Vulnerability in the Hyperion BI+ component of Oracle Hyperion (subcomponent: Foundation UI & Servlets). The supported version that is affected is 11.1.2.4. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Hyperion BI+. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Hyperion BI+ accessible data as well as unauthorized read access to a subset of Hyperion BI+ accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Hyperion BI+. CVSS 3.0 Base Score 4.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/ C:L/I:L/A:L). **CVE ID : CVE-2018-2594**	http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html	A-ORA-HYPER-010218/87
Hyperion Data Relationship Management					

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	Patch	NCIIPC ID
Gain Information	17-01-2018	5	Vulnerability in the Hyperion Data Relationship Management component of Oracle Hyperion (subcomponent: Access and security). The supported version that is affected is 11.1.2.4.330. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Hyperion Data Relationship Management. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Hyperion Data Relationship 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-2018-2610**	http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html	A-ORA-HYPER-010218/88
Hyperion Planning					
NA	17-01-2018	4.6	Vulnerability in the Oracle Hyperion Planning component of Oracle Hyperion (subcomponent: Security). The supported version that is affected is 11.1.2.4.007. Difficult to exploit vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Hyperion Planning. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Hyperion Planning, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle Hyperion Planning. CVSS 3.0 Base Score 7.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:C/C:H/I:H/A:H). **CVE ID : CVE-2018-2733**	http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html	A-ORA-HYPER-010218/89
Internet Directory					
NA	17-01-2018	6	Vulnerability in the Oracle Internet	http://www.	A-ORA-

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Directory component of Oracle Fusion Middleware (subcomponent: Oracle Directory Services Manager). Supported versions that are affected are 11.1.1.7.0, 11.1.1.9.0 and 12.2.1.3.0. Difficult to exploit vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Internet Directory. While the vulnerability is in Oracle Internet Directory, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle Internet Directory. CVSS 3.0 Base Score 8.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H). **CVE ID : CVE-2018-2601**	oracle.com/technetwork/security-advisory/cpujan2018-3236628.html	INTER-010218/90
Jd Edwards Enterpriseone Tools					
NA	17-01-2018	5.8	Vulnerability in the JD Edwards EnterpriseOne Tools component of Oracle JD Edwards Products (subcomponent: Web Runtime SEC). 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	http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html	A-ORA-JDED-010218/91

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2018-2659**		
NA	17-01-2018	5.8	Vulnerability in the JD Edwards EnterpriseOne Tools component of Oracle JD Edwards Products (subcomponent: Web Runtime SEC). The supported version that is affected is 9.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise JD Edwards EnterpriseOne Tools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in JD Edwards EnterpriseOne Tools, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of JD Edwards EnterpriseOne Tools accessible data as well as unauthorized read access to a subset of JD Edwards EnterpriseOne Tools accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2018-2658**	http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html	A-ORA-JDED-010218/92
Jdeveloper					
DoS Directory Traversal.	17-01-2018	3.7	Vulnerability in the Oracle JDeveloper component of Oracle Fusion Middleware (subcomponent: Deployment). Supported versions that are affected are 11.1.1.7.0, 11.1.1.7.1, 11.1.1.9.0, 11.1.2.4.0, 12.1.3.0.0 and 12.2.1.2.0. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle JDeveloper	http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html	A-ORA-JDEVE-010218/93

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			executes to compromise Oracle JDeveloper. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle JDeveloper, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle JDeveloper accessible data as well as unauthorized read access to a subset of Oracle JDeveloper accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle JDeveloper. CVSS 3.0 Base Score 4.7 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:H/UI:R/S:C/C:L/I:L/A:L). **CVE ID : CVE-2017-10273**		
NA	17-01-2018	5.8	Vulnerability in the Oracle JDeveloper component of Oracle Fusion Middleware (subcomponent: Security Framework). Supported versions that are affected are 11.1.1.2.4, 11.1.1.7.0, 11.1.1.7.1, 11.1.1.9.0 and 12.1.3.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle JDeveloper. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle JDeveloper, 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 JDeveloper accessible data as well as unauthorized update, insert or delete access to some of Oracle JDeveloper accessible data. CVSS 3.0 Base Score 8.2	http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html	A-ORA-JDEVE-010218/94

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	Patch	NCIIPC ID
			(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-2018-2711**		
JDK;JRE					
NA	17-01-2018	3.7	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: Installer). Supported versions that are affected are Java SE: 8u152 and 9.0.1. Difficult to exploit vulnerability allows low privileged attacker with logon to the infrastructure where Java SE executes 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: This vulnerability applies to the Windows installer only. CVSS 3.0 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:C/C:H/I:H/A:H). **CVE ID : CVE-2018-2627**	http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html	A-ORA-JDK;J-010218/95
DoS Execute Code	17-01-2018	3.7	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: I18n). Supported versions that are affected are Java SE: 6u171, 7u161, 8u152 and 9.0.1; Java SE Embedded: 8u151. Difficult to exploit vulnerability allows unauthenticated attacker with logon to the infrastructure where Java SE, Java SE Embedded executes 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 update,	https://security.netapp.com/advisory/ntap-20180117-0001/	A-ORA-JDK;J-010218/96

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			insert or delete access to some of Java SE, Java SE Embedded accessible data as well as unauthorized read access to a subset of Java SE, Java SE Embedded accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. 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 4.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:U/ C:L/I:L/A:L). **CVE ID : CVE-2018-2602**		
DoS	17-01-2018	4.3	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: AWT). Supported versions that are affected are Java SE: 6u171, 7u161, 8u152 and 9.0.1; Java SE Embedded: 8u151. Easily exploitable 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. 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. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start	https://security.netapp.com/advisory/ntap-20180117-0001/	A-ORA-JDK;J-010218/97

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/ C:N/I:N/A:L). **CVE ID : CVE-2018-2677**		
Gain Information	17-01-2018	4.3	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: JGSS). Supported versions that are affected are Java SE: 7u161, 8u152 and 9.0.1; Java SE Embedded: 8u151. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. While the vulnerability is in Java SE, Java SE Embedded, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to 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 6.8 (Confidentiality impacts). CVSS Vector:	https://security.netapp.com/advisory/ntap-20180117-0001/	A-ORA-JDK;J-010218/98

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:N/A:N). **CVE ID : CVE-2018-2634**		
NA	17-01-2018	4.3	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Hotspot). Supported versions that are affected are Java SE: 8u152 and 9.0.1; Java SE Embedded: 8u151. Easily exploitable 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. 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 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 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-2018-2582**	http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html	A-ORA-JDK;J-010218/99
Gain Information	17-01-2018	4.3	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: JavaFX). Supported versions that are affected are Java SE: 7u161, 8u152 and 9.0.1. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful	http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html	A-ORA-JDK;J-010218/100

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 unauthorized read access to a subset of Java SE 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 4.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:N/A:N). **CVE ID : CVE-2018-2581**		
NA	17-01-2018	5.1	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: Deployment). Supported versions that are affected are Java SE: 8u152 and 9.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, attacks may significantly impact additional 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,	http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html	A-ORA-JDK;J-010218/101

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2018-2638**		
NA	17-01-2018	6.8	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: Deployment). Supported versions that are affected are Java SE: 8u152 and 9.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 8.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/	http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html	A-ORA-JDK;J-010218/102

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	Patch	NCIIPC ID
			C:H/I:H/A:H). **CVE ID : CVE-2018-2639**		
JDK;JRE;Jrockit					
Gain Information	17-01-2018	4	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: LDAP). Supported versions that are affected are Java SE: 6u171, 7u161, 8u152 and 9.0.1; Java SE Embedded: 8u151; JRockit: R28.3.16. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE, Java SE Embedded, JRockit accessible data. Note: This vulnerability 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 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-2018-2588**	https://security.netapp.com/advisory/ntap-20180117-0001/	A-ORA-JDK;J-010218/103
DoS	17-01-2018	4.3	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: JNDI). Supported versions that are affected are Java SE: 6u171, 7u161, 8u152 and 9.0.1; Java SE Embedded: 8u151; JRockit: R28.3.16. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java	https://security.netapp.com/advisory/ntap-20180117-0001/	A-ORA-JDK;J-010218/104

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	Patch	NCIIPC ID
			SE, Java SE Embedded, JRockit. Successful attacks require human interaction from a person other than the attacker. 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: This vulnerability 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 4.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/ C:N/I:N/A:L). **CVE ID : CVE-2018-2678**		
DoS	17-01-2018	4.3	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: Libraries). Supported versions that are affected are Java SE: 6u171, 7u161, 8u152 and 9.0.1; Java SE Embedded: 8u151; JRockit: R28.3.16. Easily exploitable vulnerability allows 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. 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: This vulnerability applies to client and server deployment of Java.	http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html	A-ORA-JDK;J-010218/105

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	Patch	NCIIPC ID
			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 4.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/ C:N/I:N/A:L). **CVE ID : CVE-2018-2663**		
NA	17-01-2018	4.3	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: JCE). Supported versions that are affected are Java SE: 6u171, 7u161, 8u152 and 9.0.1; Java SE Embedded: 8u151; JRockit: R28.3.16. 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 access to critical data or complete access to all Java SE, Java SE Embedded, JRockit accessible data. Note: This vulnerability applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 5.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/	https://security.netapp.com/advisory/ntap-20180117-0001/	A-ORA-JDK;J-010218/106

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			C:H/I:N/A:N). **CVE ID : CVE-2018-2618**		
Gain Information	17-01-2018	4.3	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: Libraries). Supported versions that are affected are Java SE: 6u171, 7u161, 8u152 and 9.0.1; Java SE Embedded: 8u151; JRockit: R28.3.16. 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 read access to a subset of Java SE, Java SE Embedded, JRockit accessible data. Note: This vulnerability 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 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2018-2579**	https://security.netapp.com/advisory/ntap-20180117-0001/	A-ORA-JDK;J-010218/107
DoS	17-01-2018	5	Vulnerability in the Java SE, JRockit component of Oracle Java SE (subcomponent: Serialization). Supported versions that are affected are Java SE: 6u171 and 7u161; JRockit: R28.3.16. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, JRockit. Successful attacks of this	https://security.netapp.com/advisory/ntap-20180117-0001/	A-ORA-JDK;J-010218/108

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, JRockit. 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. 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-2018-2657**		
DoS	17-01-2018	5	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: Libraries). Supported versions that are affected are Java SE: 6u171, 7u161, 8u152 and 9.0.1; Java SE Embedded: 8u151; JRockit: R28.3.16. 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 Embedded, JRockit. Note: This vulnerability 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 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/	https://security.netapp.com/advisory/ntap-20180117-0001/	A-ORA-JDK;J-010218/109

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	Patch	NCIIPC ID
			C:N/I:N/A:L). **CVE ID : CVE-2018-2603**		
NA	17-01-2018	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: 6u171, 7u161, 8u152 and 9.0.1; Java SE Embedded: 8u151; JRockit: R28.3.16. Difficult to exploit vulnerability allows 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 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 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-2018-2633**	https://security.netapp.com/advisory/ntap-20180117-0001/	A-ORA-JDK;J-010218/110
NA	17-01-2018	5.8	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: JMX). Supported versions that are affected are Java SE: 6u171, 7u161, 8u152 and 9.0.1; Java SE Embedded: 8u151;	http://www.oracle.com/technetwork/security-advisory/cpujan2018-	A-ORA-JDK;J-010218/111

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	Patch	NCIIPC ID
			JRockit: R28.3.16. 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 creation, deletion or modification access to critical data or all Java SE, Java SE Embedded, JRockit accessible data as well as unauthorized access to critical data or complete access to all Java SE, Java SE Embedded, JRockit accessible data. 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. CVSS 3.0 Base Score 7.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N). **CVE ID : CVE-2018-2637**	3236628.html	
DoS	17-01-2018	5.8	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: JNDI). Supported versions that are affected are Java SE: 6u171, 7u161, 8u152 and 9.0.1; Java SE Embedded: 8u151; JRockit: R28.3.16. 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 update, insert or delete access to some 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	https://security.netapp.com/advisory/ntap-20180117-0001/	A-ORA-JDK;J-010218/112

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	Patch	NCIIPC ID
			vulnerability 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 4.8 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:L). **CVE ID : CVE-2018-2599**		
Mysql					
Gain Information	17-01-2018	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Performance Schema). Supported versions that are affected are 5.6.38 and prior and 5.7.20 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 access to critical data or complete access to all MySQL Server accessible data. CVSS 3.0 Base Score 4.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2018-2645**	http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html	A-ORA-MYSQL-010218/113
NA	17-01-2018	6.8	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server : Security : Privileges). Supported versions that are affected are 5.6.38 and prior and 5.7.20 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise	https://security.netapp.com/advisory/ntap-20180117-0002/	A-ORA-MYSQL-010218/114

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2018-2703**		
NA	17-01-2018	6.8	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.5.58 and prior, 5.6.38 and prior and 5.7.20 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-2018-2668**	https://security.netapp.com/advisory/ntap-20180117-0002/	A-ORA-MYSQL-010218/115
NA	17-01-2018	6.8	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.7.20 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-2018-2667**	https://security.netapp.com/advisory/ntap-20180117-0002/	A-ORA-MYSQL-010218/116

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	Patch	NCIIPC ID
NA	17-01-2018	6.8	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.5.58 and prior, 5.6.38 and prior and 5.7.20 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-2018-2665**	http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html	A-ORA-MYSQL-010218/117
NA	17-01-2018	6.8	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DML). Supported versions that are affected are 5.7.20 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-2018-2646**	https://security.netapp.com/advisory/ntap-20180117-0002/	A-ORA-MYSQL-010218/118
NA	17-01-2018	6.8	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.5.58 and prior, 5.6.38 and prior and 5.7.20 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise	https://security.netapp.com/advisory/ntap-20180117-0002/	A-ORA-MYSQL-010218/119

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	Patch	NCIIPC ID
			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-2018-2640**		
NA	17-01-2018	6.8	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 5.5.58 and prior, 5.6.38 and prior and 5.7.20 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-2018-2622**	https://security.netapp.com/advisory/ntap-20180117-0002/	A-ORA-MYSQL-010218/120
NA	17-01-2018	6.8	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.7.20 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).	https://security.netapp.com/advisory/ntap-20180117-0002/	A-ORA-MYSQL-010218/121

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	Patch	NCIIPC ID
			CVE ID : CVE-2018-2600		
NA	17-01-2018	6.8	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server : Partition). Supported versions that are affected are 5.6.38 and prior and 5.7.19 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-2018-2591**	https://security.netapp.com/advisory/ntap-20180117-0002/	A-ORA-MYSQL-010218/ 122
NA	17-01-2018	6.8	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Performance Schema). Supported versions that are affected are 5.6.38 and prior and 5.7.20 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-2018-2590**	https://security.netapp.com/advisory/ntap-20180117-0002/	A-ORA-MYSQL-010218/ 123
NA	17-01-2018	6.8	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DML). Supported versions that are affected are 5.7.20 and prior. Easily exploitable vulnerability allows high privileged	https://security.netapp.com/advisory/ntap-20180117-0002/	A-ORA-MYSQL-010218/ 124

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	Patch	NCIIPC ID
			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-2018-2586**		
NA	17-01-2018	6.8	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Stored Procedure). Supported versions that are affected are 5.6.38 and prior and 5.7.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. While the vulnerability is in MySQL Server, 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 MySQL Server. CVSS 3.0 Base Score 6.8 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:C/ C:N/I:N/A:H). **CVE ID : CVE-2018-2583**	https://security.netapp.com/advisory/ntap-20180117-0002/	A-ORA-MYSQL-010218/ 125
NA	17-01-2018	6.8	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DML). Supported versions that are affected are 5.7.20 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	https://security.netapp.com/advisory/ntap-20180117-0002/	A-ORA-MYSQL-010218/ 126

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2018-2576**		
NA	17-01-2018	6.8	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: GIS). Supported versions that are affected are 5.6.38 and prior and 5.7.20 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-2018-2573**	https://security.netapp.com/advisory/ntap-20180117-0002/	A-ORA-MYSQL-010218/127
NA	17-01-2018	6.8	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: InnoDB). Supported versions that are affected are 5.7.20 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-2018-2565**	https://security.netapp.com/advisory/ntap-20180117-0002/	A-ORA-MYSQL-010218/128
NA	17-01-2018	7.5	Vulnerability in the MySQL Server component of Oracle MySQL	https://security.netapp.c	A-ORA-MYSQL-

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	Patch	NCIIPC ID
			(subcomponent: Server: Replication). Supported versions that are affected are 5.6.38 and prior and 5.7.20 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 as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H). **CVE ID : CVE-2018-2647**	om/advisory/ntap-20180117-0002/	010218/129
NA	17-01-2018	7.5	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.6.38 and prior and 5.7.20 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 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-2018-2612**	https://security.netapp.com/advisory/ntap-20180117-0002/	A-ORA-MYSQL-010218/130
NA	17-01-2018	7.5	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server : Partition).	http://www.oracle.com/technetwork/	A-ORA-MYSQL-010218/

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	Patch	NCIIPC ID
			Supported versions that are affected are 5.5.58 and prior, 5.6.38 and prior and 5.7.19 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-2018-2562**	security-advisory/cpujan2018-3236628.html	131
NA	17-01-2018	7.8	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server : Security : Privileges). Supported versions that are affected are 5.6.38 and prior and 5.7.20 and prior. Easily exploitable vulnerability allows unauthenticated 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 7.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2018-2696**	https://security.netapp.com/advisory/ntap-20180117-0002/	A-ORA-MYSQL-010218/132
Mysql Connector/net					
NA	17-01-2018	7.8	Vulnerability in the MySQL Connectors component of Oracle MySQL (subcomponent: Connector/Net). Supported versions that are affected are 6.9.9 and prior and 6.10.4 and prior. Easily exploitable vulnerability allows	https://security.netapp.com/advisory/ntap-20180117-0002/	A-ORA-MYSQL-010218/133

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated attacker with network access via multiple protocols to compromise MySQL Connectors. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Connectors. CVSS 3.0 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2018-2585**		
Peoplesoft Enterprise Human Capital Management Human Resources					
NA	17-01-2018	4.9	Vulnerability in the PeopleSoft Enterprise HCM Human Resources component of Oracle PeopleSoft Products (subcomponent: Security). The supported version that is affected is 9.2. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise HCM Human Resources. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise HCM Human Resources accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise HCM Human Resources accessible data. CVSS 3.0 Base Score 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-2018-2681**	http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html	A-ORA-PEOPL-010218/134
NA	17-01-2018	5.8	Vulnerability in the PeopleSoft Enterprise HCM Human Resources component of Oracle PeopleSoft Products (subcomponent: Company Dir / Org Chart Viewer). The supported version that is affected is 9.2. Easily exploitable vulnerability allows unauthenticated attacker with network	http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html	A-ORA-PEOPL-010218/135

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			access via HTTP to compromise PeopleSoft Enterprise HCM Human Resources. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise HCM Human Resources, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise HCM Human Resources accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise HCM Human Resources accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2018-2654**		
Peoplesoft Enterprise Peopletools					
NA	17-01-2018	4	Vulnerability in the PeopleSoft Enterprise PeopleTools component of Oracle PeopleSoft Products (subcomponent: Query). Supported versions that are affected are 8.54, 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 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:L/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2018-2695**	http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html	A-ORA-PEOPL-010218/136
Gain Information	17-01-2018	4	Vulnerability in the PeopleSoft Enterprise PeopleTools component of	http://www.oracle.com/t	A-ORA-PEOPL-

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Oracle PeopleSoft Products (subcomponent: Integration Broker). Supported versions that are affected are 8.54, 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 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:L/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2018-2605**	echnetwork/security-advisory/cpujan2018-3236628.html	010218/137
Gain Information	17-01-2018	5	Vulnerability in the PeopleSoft Enterprise PeopleTools component of Oracle PeopleSoft Products (subcomponent: Connected Query). Supported versions that are affected are 8.54, 8.55 and 8.56. Easily exploitable vulnerability allows unauthenticated 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 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-2018-2653**	http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html	A-ORA-PEOPL-010218/138
Gain Information	17-01-2018	5	Vulnerability in the PeopleSoft Enterprise PeopleTools component of Oracle PeopleSoft Products (subcomponent: Integration Broker). Supported versions that are affected are 8.54, 8.55 and 8.56. Easily exploitable vulnerability allows	http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.ht	A-ORA-PEOPL-010218/139

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	Patch	NCIIPC ID
			unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. 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 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-2018-2652**	ml	
Gain Information	17-01-2018	5	Vulnerability in the PeopleSoft Enterprise PeopleTools component of Oracle PeopleSoft Products (subcomponent: XML Publisher). Supported versions that are affected are 8.54, 8.55 and 8.56. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. 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 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-2018-2651**	http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html	A-ORA-PEOPL-010218/140
NA	17-01-2018	5.5	Vulnerability in the PeopleSoft Enterprise PRTL Interaction Hub component of Oracle PeopleSoft Products (subcomponent: Enterprise Portal). The supported version that is affected is 9.1.00. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise PRTL Interaction Hub. Successful attacks of this vulnerability can result in unauthorized creation, deletion or	http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html	A-ORA-PEOPL-010218/141

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	Patch	NCIIPC ID
			modification access to critical data or all PeopleSoft Enterprise PRTL Interaction Hub accessible data as well as unauthorized access to critical data or complete access to all PeopleSoft Enterprise PRTL Interaction Hub 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-2017-10301**		
NA	17-01-2018	6.8	Vulnerability in the PeopleSoft Enterprise PeopleTools component of Oracle PeopleSoft Products (subcomponent: PIA Core Technology). Supported versions that are affected are 8.54, 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 takeover of PeopleSoft Enterprise PeopleTools. CVSS 3.0 Base Score 8.8 (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:H). **CVE ID : CVE-2018-2593**	http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html	A-ORA-PEOPL-010218/142
Peoplesoft Enterprise Scm Eprocurement					
NA	17-01-2018	5.5	Vulnerability in the PeopleSoft Enterprise SCM eProcurement component of Oracle PeopleSoft Products (subcomponent: Manage Requisition Status). Supported versions that are affected are 9.1 and 9.2. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft	http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html	A-ORA-PEOPL-010218/143

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	Patch	NCIIPC ID
			Enterprise SCM eProcurement. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise SCM eProcurement accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise SCM eProcurement 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-2018-2731**		
Peoplesoft Enterprise Scm Purchasing					
Gain Information	17-01-2018	4	Vulnerability in the PeopleSoft Enterprise SCM Purchasing component of Oracle PeopleSoft Products (subcomponent: Supplier Registration). The supported version that is affected is 9.2. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise SCM Purchasing. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all PeopleSoft Enterprise SCM Purchasing 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-2018-2671**	http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html	A-ORA-PEOPL-010218/144
Peoplesoft Enterprise Scm Strategic Sourcing					
Gain Information	17-01-2018	4	Vulnerability in the PeopleSoft Enterprise FSCM component of Oracle PeopleSoft Products (subcomponent: Strategic Sourcing). The supported version that is affected is 9.2. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft	http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html	A-ORA-PEOPL-010218/145

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Enterprise FSCM. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all PeopleSoft Enterprise FSCM 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-2018-2702**		
Retail Merchandising System					
NA	17-01-2018	5.5	Vulnerability in the Oracle Retail Merchandising System component of Oracle Retail Applications (subcomponent: Cross Pillar). The supported version that is affected is 16.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Retail Merchandising System. While the vulnerability is in Oracle Retail Merchandising System, 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 Merchandising System accessible data as well as unauthorized read access to a subset of Oracle Retail Merchandising System accessible data. CVSS 3.0 Base Score 6.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:N). **CVE ID : CVE-2018-2730**	http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html	A-ORA-RETAI-010218/146
Siebel Customer Relationship Management Desktop					
NA	17-01-2018	5.5	Vulnerability in the Siebel CRM Desktop component of Oracle Siebel CRM (subcomponent: Outlook Client). Supported versions that are affected are 16.0 and 17.0. Easily exploitable vulnerability allows low privileged	http://www.oracle.com/technetwork/security-advisory/cpujan2018-	A-ORA-SIEBE-010218/147

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker with network access via HTTP to compromise Siebel CRM Desktop. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Siebel CRM Desktop accessible data as well as unauthorized access to critical data or complete access to all Siebel CRM Desktop 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-2018-2574**	3236628.html	
Siebel Engineering-installer And Deployment					
Gain Information	17-01-2018	4	Vulnerability in the Siebel Engineering - Installer and Deployment component of Oracle Siebel CRM (subcomponent: Siebel Approval Manager). Supported versions that are affected are 16.0 and 17.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Siebel Engineering - Installer and Deployment. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Siebel Engineering - Installer and Deployment 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-2018-2632**	http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html	A-ORA-SIEBE-010218/148
Transportation Management					
Gain Information	17-01-2018	4	Vulnerability in the Oracle Transportation Management component of Oracle Supply Chain Products Suite (subcomponent: Security). Supported versions that are affected are 6.2.11, 6.3.1, 6.3.2, 6.3.3, 6.3.4, 6.3.5, 6.3.6, 6.3.7, 6.4.1, 6.4.2 and	http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.ht	A-ORA-TRANS-010218/149

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			6.4.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Transportation Management. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Transportation 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-2018-2631**	ml	
NA	17-01-2018	5.5	Vulnerability in the Oracle Transportation Management component of Oracle Supply Chain Products Suite (subcomponent: Security). Supported versions that are affected are 6.2.11, 6.3.1, 6.3.2, 6.3.3, 6.3.4, 6.3.5, 6.3.6, 6.3.7 and 6.4.1. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Transportation Management. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Transportation Management accessible data as well as unauthorized read access to a subset of Oracle Transportation 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-2018-2662**	http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html	A-ORA-TRANS-010218/150
User Management					
NA	17-01-2018	5.5	Vulnerability in the Oracle User Management component of Oracle E-Business Suite (subcomponent: Proxy User Delegation). Supported versions that are affected are 12.1.3, 12.2.3,	http://www.oracle.com/technetwork/security-advisory/cp	A-ORA-USER -010218/151

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			12.2.4, 12.2.5, 12.2.6 and 12.2.7. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle User Management. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle User Management accessible data as well as unauthorized read access to a subset of Oracle User 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-2018-2691**	ujan2018-3236628.html	
Vm Virtualbox					
NA	17-01-2018	4.1	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are Prior to 5.1.32 and Prior to 5.2.6. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. 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 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H). **CVE ID : CVE-2018-2698**	http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html	A-ORA-VM VI-010218/152
NA	17-01-2018	4.1	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are Prior to 5.1.32 and Prior to 5.2.6.	http://www.oracle.com/technetwork/security-advisory/cp	A-ORA-VM VI-010218/153

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	Patch	NCIIPC ID
			Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. 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 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H). **CVE ID : CVE-2018-2694**	ujan2018-3236628.html	
NA	17-01-2018	4.1	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Guest Additions). Supported versions that are affected are Prior to 5.1.32 and Prior to 5.2.6. Easily exploitable vulnerability allows low privileged 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 8.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:H). **CVE ID : CVE-2018-2693**	http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html	A-ORA-VM VI-010218/154
NA	17-01-2018	4.3	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected	http://www.oracle.com/technetwork/security-	A-ORA-VM VI-010218/155

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			are Prior to 5.1.32 and Prior to 5.2.6. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. 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 8.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H). **CVE ID : CVE-2018-2676**	advisory/cpujan2018-3236628.html	
NA	17-01-2018	4.4	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are Prior to 5.1.32 and Prior to 5.2.6. 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-2018-2690**	http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html	A-ORA-VM VI-010218/156
NA	17-01-2018	4.4	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core).	http://www.oracle.com/technetwork/	A-ORA-VM VI-010218/157

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	Patch	NCIIPC ID
			Supported versions that are affected are Prior to 5.1.32 and Prior to 5.2.6. 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-2018-2689**	security-advisory/cpujan2018-3236628.html	
NA	17-01-2018	4.4	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are Prior to 5.1.32 and Prior to 5.2.6. 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-2018-2688**	http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html	A-ORA-VM VI-010218/158

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	Patch	NCIIPC ID
NA	17-01-2018	4.4	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are Prior to 5.1.32 and Prior to 5.2.6. 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-2018-2687**	http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html	A-ORA-VM VI-010218/159
NA	17-01-2018	4.4	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are Prior to 5.1.32 and Prior to 5.2.6. 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:	http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html	A-ORA-VM VI-010218/160

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	Patch	NCIIPC ID
			(CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H). **CVE ID : CVE-2018-2686**		
NA	17-01-2018	4.4	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are Prior to 5.1.32 and Prior to 5.2.6. 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-2018-2685**	http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html	A-ORA-VMVI-010218/161
Webcenter Content					
NA	17-01-2018	5.8	Vulnerability in the Oracle WebCenter Content component of Oracle Fusion Middleware (subcomponent: Content Server). 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 Content. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle WebCenter Content, attacks may significantly impact additional products. Successful attacks of this vulnerability can result	http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html	A-ORA-WEBCE-010218/162

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	Patch	NCIIPC ID
			in unauthorized creation, deletion or modification access to critical data or all Oracle WebCenter Content accessible data as well as unauthorized read access to a subset of Oracle WebCenter Content 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:L/I:H/A:N). **CVE ID : CVE-2018-2596**		
Webcenter Content					
NA	17-01-2018	5.8	Vulnerability in the Oracle WebCenter Content component of Oracle Fusion Middleware (subcomponent: Content Server). The supported version that is affected is 11.1.1.9.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebCenter Content. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle WebCenter Content, 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 WebCenter Content accessible data as well as unauthorized read access to a subset of Oracle WebCenter Content 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:L/I:H/A:N). **CVE ID : CVE-2018-2564**	http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html	A-ORA-WEBCE-010218/163
Webcenter Portal					
NA	17-01-2018	5.8	Vulnerability in the Oracle WebCenter Portal component of Oracle Fusion Middleware (subcomponent: WebCenter Spaces Application).	http://www.oracle.com/technetwork/security-	A-ORA-WEBCE-010218/164

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 require human interaction from a person other than the attacker and while the vulnerability is in Oracle WebCenter Portal, 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 WebCenter Portal accessible data as well as unauthorized read access to a subset of Oracle WebCenter Portal 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:L/I:H/A:N). **CVE ID : CVE-2018-2713**	advisory/cpujan2018-3236628.html	
Webcenter Sites					
Gain Information	17-01-2018	4	Vulnerability in the Oracle WebCenter Sites component of Oracle Fusion Middleware (subcomponent: Advanced UI). The supported version that is affected is 11.1.1.8.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle WebCenter Sites. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle WebCenter Sites 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-2018-2584**	http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html	A-ORA-WEBCE-010218/165
Weblogic Server					
Gain	17-01-2018	5	Vulnerability in the Oracle WebLogic	http://www.	A-ORA-

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information			Server component of Oracle Fusion Middleware (subcomponent: Web Services). Supported versions that are affected are 12.1.3.0.0, 12.2.1.3.0 and 12.2.1.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle WebLogic Server 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-2018-2625**	oracle.com/technetwork/security-advisory/cpujan2018-3236628.html	WEBLO-010218/166
Work In Process					
NA	17-01-2018	6.4	Vulnerability in the Oracle Work in Process component of Oracle E-Business Suite (subcomponent: Assemble/Configure to Order). 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 Work in Process. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Work in Process accessible data as well as unauthorized access to critical data or complete access to all Oracle Work in Process accessible data. CVSS 3.0 Base Score 9.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/ C:H/I:H/A:N). **CVE ID : CVE-2018-2655**	http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html	A-ORA-WORK - 010218/167
Podofo Project					
Podofo					
DoS	19-01-2018	4.3	In PoDoFo 0.9.5, there is an	https://bugz	A-POD-

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	Patch	NCIIPC ID
			uncontrolled memory allocation in the PoDoFo::PdfVecObjects::Reserve function (base/PdfVecObjects.h). Remote attackers could leverage this vulnerability to cause a denial of service via a crafted pdf file. **CVE ID : CVE-2018-5783**	illa.redhat.com/show_bug.cgi?id=1536179	PODOF-010218/168
Rails Admin Project					
Rails Admin					
XSS	19-01-2018	4.3	An exploitable cross site scripting (XSS) vulnerability exists in the add filter functionality of the rails_admin rails gem version 1.2.0. A specially crafted URL can cause an XSS flaw resulting in an attacker being able to execute arbitrary javascript on the victim's browser. An attacker can phish an authenticated user to trigger this vulnerability. **CVE ID : CVE-2017-12098**	NA	A-RAI-RAILS-010218/169
Samba					
Rsync					
Bypass	17-01-2018	5	The parse_arguments function in options.c in rsyncd in rsync before 3.1.3 does not prevent multiple --protect-args uses, which allows remote attackers to bypass an argument-sanitization protection mechanism. **CVE ID : CVE-2018-5764**	https://git.samba.org/rsync.git/?p=rsync.git;a=commit;h=7706303828fcde524222babb2833864a4bd09e07	A-SAM-RSYNC-010218/170
Sugarcrm					
Sugarcrm					
XSS	16-01-2018	4.3	phprint.php in SugarCRM 3.5.1 has XSS via a parameter name in the query string (aka a $key variable). **CVE ID : CVE-2018-5715**	NA	A-SUG-SUGAR-010218/171
Synocor					
Zimbra Collaboration Suite					
XSS	16-01-2018	3.5	Cross-site scripting (XSS) vulnerability in Zimbra Collaboration Suite (aka ZCS) before 8.8.0 Beta2 might allow remote	https://wiki.zimbra.com/wiki/Zimbra	A-SYN-ZIMBR-010218/

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attackers to inject arbitrary web script or HTML via vectors related to the "Show Snippet" functionality. **CVE ID : CVE-2017-8802**	_Security_Advisories	172
Trendmicro					
Mobile Security					
Gain Information	19-01-2018	5	An uninitialized pointer information disclosure vulnerability in Trend Micro Mobile Security (Enterprise) versions 9.7 and below could allow an unauthenticated remote attacker to disclosure sensitive information on a vulnerable system. **CVE ID : CVE-2017-14082**	https://success.trendmicro.com/solution/1118993	A-TRE-MOBIL-010218/173
Smart Protection Server					
XSS	19-01-2018	4.3	A stored cross site scripting (XSS) vulnerability in Trend Micro Smart Protection Server (Standalone) versions 3.2 and below could allow an attacker to execute a malicious payload on vulnerable systems. **CVE ID : CVE-2017-14096**	https://success.trendmicro.com/solution/1118992	A-TRE-SMART-010218/174
NA	19-01-2018	5	An improper access control vulnerability in Trend Micro Smart Protection Server (Standalone) versions 3.2 and below could allow an attacker to decrypt contents of a database with information that could be used to access a vulnerable system. **CVE ID : CVE-2017-14097**	https://success.trendmicro.com/solution/1118992	A-TRE-SMART-010218/175
Execute Code File Inclusion	19-01-2018	6.8	A vulnerability in Trend Micro Smart Protection Server (Standalone) versions 3.2 and below could allow an attacker to perform remote command execution via a local file inclusion on a vulnerable system. **CVE ID : CVE-2017-14095**	https://success.trendmicro.com/solution/1118992	A-TRE-SMART-010218/176
Execute Code	19-01-2018	7.5	A vulnerability in Trend Micro Smart Protection Server (Standalone) versions 3.2 and below could allow an attacker to perform remote command execution via a cron job injection on a vulnerable system.	https://success.trendmicro.com/solution/1118992	A-TRE-SMART-010218/177

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2017-14094		
Wondercms					
Wondercms					
NA	2018-01-26	6.5	In WonderCMS 2.3.1, the upload functionality accepts random application extensions and leads to malicious File Upload. **CVE ID : CVE-2017-14521**	https://securitywarrior9.blogspot.in/2018/01/vulnerability-in-wonder-cms-leading-to.html	A-WON-WONDE-010218/178
Wordpress					
Wordpress					
XSS	18-01-2018	4.3	WordPress before 4.9.2 has XSS in the Flash fallback files in MediaElement (under wp-includes/js/mediaelement). **CVE ID : CVE-2018-5776**	https://wordpress.org/news/2018/01/wordpress-4-9-2-security-and-maintenance-release/	A-WOR-WORDP-010218/179
Yandex					
Yandex Browser					
Memory Corruption	19-01-2018	5.1	Race condition issue in Yandex Browser for Android before 17.4.0.16 allowed a remote attacker to potentially exploit memory corruption via a crafted HTML page **CVE ID : CVE-2017-7326**	https://browser.yandex.com/security/changelogs/fixed-in-version-17-4	A-YAN-YANDE-010218/180
NA	19-01-2018	6.8	Yandex Browser installer for Desktop before 17.4.1 has a DLL Hijacking Vulnerability because an untrusted search path is used for dnsapi.dll, winmm.dll, ntmarta.dll, cryptbase.dll or profapi.dll. **CVE ID : CVE-2017-7327**	https://browser.yandex.com/security/changelogs/fixed-in-version-17-4	A-YAN-YANDE-010218/181
OPERATING SYSTEM(OS)					
Asuswrt-merlin Project					
Asuswrt-merlin					
Execute Code Overflow	17-01-2018	6.5	Stack-based buffer overflow in the ej_update_variables function in	http://www.w0lfzhang.co	O-ASU-ASUSW-

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	Patch	NCIIPC ID
			router/httpd/web.c on ASUS routers (when using software from https://github.com/RMerl/asuswrt-merlin) allows web authenticated attackers to execute code via a request that updates a setting. In ej_update_variables, the length of the variable action_script is not checked, as long as it includes a "_wan_if" substring. **CVE ID : CVE-2018-5721**	m/2018/01/17/ASUS-router-stack-overflow-in-http-server/	010218/182
Cobham					
Seatel 121 Firmware					
Gain Information	16-01-2018	5	Cobham Sea Tel 121 build 222701 devices allow remote attackers to obtain potentially sensitive information via a /cgi-bin/getSysStatus request, as demonstrated by the Latitude/Longitude of the ship, or satellite details. **CVE ID : CVE-2018-5728**	http://misteralfa-hack.blogspot.cl/2018/01/seatelcobham-donde-esta-mi-barco.html	O-COB-SEATE-010218/183
Google					
Android					
Overflow	16-01-2018	4.6	In Android for MSM, Firefox OS for MSM, QRD Android, with all Android releases from CAF using the Linux kernel, while calculating CRC for GPT header fields with partition entries greater than 16384 buffer overflow occurs. **CVE ID : CVE-2017-11072**	https://source.android.com/security/bulletin/pixel/2018-01-01	O-GOO-ANDRO-010218/184
Linux					
Linux Kernel					
DoS	16-01-2018	7.1	In the Linux kernel 4.12, 3.10, 2.6 and possibly earlier versions a race condition vulnerability exists in the sound system, this can lead to a deadlock and denial of service condition. **CVE ID : CVE-2018-1000004**	http://seclists.org/oss-sec/2018/q1/51	O-LIN-LINUX-010218/185
Oracle					
Solaris					
NA	17-01-2018	6.2	Vulnerability in the Solaris component of Oracle Sun Systems Products Suite	http://www.oracle.com/t	O-ORA-SOLAR-

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	Patch	NCIIPC ID
			(subcomponent: Kernel). The supported version that is affected is 11.3. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Solaris executes to compromise Solaris. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Solaris, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Solaris. CVSS 3.0 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:H/UI:R/S:C/C:H/I:H/A:H). **CVE ID : CVE-2018-2578**	echnetwork/security-advisory/cpujan2018-3236628.html	010218/186
NA	17-01-2018	7.8	Vulnerability in the Solaris component of Oracle Sun Systems Products Suite (subcomponent: Kernel). The supported version that is affected is 10. Easily exploitable vulnerability allows unauthenticated attacker with network access via ICMP 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. CVSS 3.0 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2018-2710**	http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html	O-ORA-SOLAR-010218/187
NA	17-01-2018	3.3	Vulnerability in the Solaris component of Oracle Sun Systems Products Suite (subcomponent: SPARC Platform). 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	http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html	O-ORA-SOLAR-010218/188

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 6.6 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N). **CVE ID : CVE-2018-2717**		