Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Application (A)					
Apache					
Derby					
NA	23-10-2017	5	In Apache Derby 10.1.2.1, 10.2.2.0, 10.3.1.4, and 10.4.1.3, Export processing may allow an attacker to overwrite an existing file. **CVE ID: CVE-2010-2232**	http://db.apache.org/derby/releases/release-10.6.2.1.html#Note+for+DERBY-2925	A-APA-DERBY-011117/1
Apple					
Apple Support					
Gain Information	22-10-2017	5	An issue was discovered in certain Apple products. The Apple Support app before 1.2 for iOS is affected. The issue involves the "Analytics" component. It allows remote attackers to obtain sensitive analytics information by leveraging its presence in a cleartext HTTP transmission to an Adobe Marketing Cloud server operated for Apple, as demonstrated by information about the installation date and time. **CVE ID: CVE-2017-7147**	https://support.apple.com/HT208201	A-APP-APPLE-011117/2
Itunes					
NA	22-10-2017	4.3	An issue was discovered in certain Apple products. iTunes before 12.7 is affected. The issue involves the "Data Sync" component. It allows attackers to access iOS backups (written by iTunes) via a crafted app. **CVE ID: CVE-2017-7079**	https://support.apple.com/HT208140	A-APP-ITUNE-011117/3
Safari					
Bypass Gain Information	22-10-2017	5	An issue was discovered in certain Apple products. Safari before 11 is affected. The issue involves the	https://support.apple.com/	A-APP-SAFAR-011117/4

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			"WebKit Storage" component. It allows attackers to bypass the Safari Private Browsing protection mechanism, and consequently obtain sensitive information about visited web sites. **CVE ID: CVE-2017-7142**	HT208116	
Xcode					
DoS Execute Code Overflow Mem. Corr.	22-10-2017	6.8	An issue was discovered in certain Apple products. Xcode before 9 is affected. The issue involves the "ld64" component. It allows remote attackers to Execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted Mach-O file. **CVE ID : CVE-2017-7137**	https://support.apple.com/HT208103	A-APP-XCODE-011117/5
DoS Execute Code Overflow Mem. Corr.	22-10-2017	6.8	An issue was discovered in certain Apple products. Xcode before 9 is affected. The issue involves the "ld64" component. It allows remote attackers to Execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted Mach-O file. **CVE ID : CVE-2017-7136**	https://support.apple.com/HT208103	A-APP-XCODE-011117/6
DoS Execute Code Overflow Mem. Corr.	22-10-2017	6.8	An issue was discovered in certain Apple products. Xcode before 9 is affected. The issue involves the "ld64" component. It allows remote attackers to Execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted Mach-O file. **CVE ID : CVE-2017-7135**	https://support.apple.com/HT208103	A-APP-XCODE-011117/7
DoS Execute Code Overflow Mem. Corr.	22-10-2017	6.8	An issue was discovered in certain Apple products. Xcode before 9 is affected. The issue involves the "ld64" component. It allows remote attackers to Execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted	https://support.apple.com/HT208103	A-APP-XCODE-011117/8

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mach-O file. **CVE ID : CVE-2017-7134**		
Artifex					
Mupdf					
Overflow	18-10-2017	6.8	An integer overflow was discovered in pdf_read_new_xref_section in pdf/pdf-xref.c in Artifex MuPDF 1.11. **CVE ID : CVE-2017-15587**	http://git.ghostscript.com/?p=mupdf.git;h=82df2631d7d0446b206ea6b434ea609b6c28b0e8	A-ART-MUPDF-011117/9
Busybox					
Busybox					
NA	24-10-2017	4.3	archival/libarchive/decompress_unlzma.c in BusyBox 1.27.2 has an Integer Underflow that leads to a read access violation. **CVE ID : CVE-2017-15874**	https://bugs.busybox.net/show_bug.cgi?id=10436	A-BUS-BUSYB-011117/10
Overflow	24-10-2017	4.3	The get_next_block function in archival/libarchive/decompress_bunzip2.c in BusyBox 1.27.2 has an Integer Overflow that may lead to a write access violation. **CVE ID : CVE-2017-15873**	NA	A-BUS-BUSYB-011117/11
Ffmpeg					
Ffmpeg					
DoS	24-10-2017	4.3	Double free vulnerability in FFmpeg 3.3.4 and earlier allows remote attackers to cause a denial of service via a crafted AVI file. **CVE ID : CVE-2017-15186**	NA	A-FFM-FFMPE-011117/12
Fiyo					
Fiyo Cms					
Gain Information	16-10-2017	5	Fiyo CMS 2.0.1.8 allows remote attackers to obtain sensitive information via a direct request to the database backup file in .backup/. **CVE ID : CVE-2014-9147**	NA	A-FIY-FIYO -011117/13
Bypass	16-10-2017	7.5	Fiyo CMS 2.0.1.8 allows remote attackers to bypass intended	NA	A-FIY-FIYO -

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 restrictions and Execute the (1) "Install and Update" or (2) Backup super administrator function via the view parameter in a direct request to fiyo/dapur. **CVE ID : CVE-2014-9148**		011117/14
Flowpaper					
Flexpaper					
XSS	17-10-2017	4.3	Cross-site scripting (XSS) vulnerability in FlexPaperViewer.swf in Flexpaper before 2.3.1 allows remote attackers to inject arbitrary web script or HTML via the Swfile parameter. **CVE ID : CVE-2014-9677**	NA	A-FLO-FLEXP-011117/15
Foxitsoftware					
Foxit Reader					
DoS Execute Code Overflow	22-10-2017	6.8	Foxit Reader 8.3.2.25013 allows attackers to Execute arbitrary code or cause a denial of service via a crafted .xps file, related to "Data from Faulting Address controls subsequent Write Address starting at msvcrt!memmove+0x0000000000000158." **CVE ID : CVE-2017-15771**	NA	A-FOX-FOXIT-011117/16
Foxit Reader					
DoS Execute Code Overflow	22-10-2017	6.8	Foxit Reader 8.3.2.25013 allows attackers to Execute arbitrary code or cause a denial of service via a crafted .xps file, related to "Data from Faulting Address controls subsequent Write Address starting at frdvpr_drv!DrvQueryDriverInfo+0x000000000002c851." **CVE ID : CVE-2017-15770**	NA	A-FOX-FOXIT-011117/17
Freedesktop					
Poppler					
NA	17-10-2017	6.8	In Poppler 0.59.0, a NULL Pointer Dereference exists in the GfxImageColorMap::getGrayLine() function in GfxState.cc via a crafted	https://bugs.freedesktop.org/show_b	A-FRE-POPPL-011117/18

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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
			PDF document. **CVE ID : CVE-2017-15565**	ug.cgi?id=103016	
GNU					
Binutils					
DoS	27-10-2017	4.3	dwarf2.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, mishandles NULL files in a .debug_line file table, which allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted ELF file, related to concat_filename. NOTE: this issue is caused by an incomplete fix for CVE ID :CVE-2017-15023. **CVE ID : CVE-2017-15939**	NA	A-GNU-BINUT-011117/19
DoS Overflow	27-10-2017	5	dwarf2.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, miscalculates DW_FORM_ref_addr die refs in the case of a relocatable object file, which allows remote attackers to cause a denial of service (find_abstract_instance_name invalid memory read, segmentation fault, and application crash). **CVE ID : CVE-2017-15938**	NA	A-GNU-BINUT-011117/20
Glibc					
DoS Overflow	20-10-2017	4.3	The glob function in glob.c in the GNU C Library (aka glibc or libc6) before 2.27, when invoked with GLOB_TILDE, could skip freeing allocated memory when processing the ~ operator with a long user name, potentially leading to a denial of service (memory leak). **CVE ID : CVE-2017-15671**	https://sourceware.org/bugzilla/show_bug.cgi?id=22325	A-GNU-GLIBC-011117/21
Overflow	20-10-2017	7.5	The GNU C Library (aka glibc or libc6) before 2.27 contains an off-by-one error leading to a heap-based buffer overflow in the glob	https://sourceware.org/bugzilla/sho	A-GNU-GLIBC-011117/22

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			function in glob.c, related to the processing of home directories using the ~ operator followed by a long string. **CVE ID : CVE-2017-15670**	w_bug.cgi?id=22320	
Overflow	22-10-2017	7.5	The glob function in glob.c in the GNU C Library (aka glibc or libc6) before 2.27 contains a buffer overflow during unescaping of user names with the ~ operator. **CVE ID : CVE-2017-15804**	https://sourceware.org/bugzilla/show_bug.cgi?id=22332	A-GNU-GLIBC-011117/23
Libextractor					
NA	26-10-2017	4.3	In GNU Libextractor 1.4, there is an out-of-bounds read in the EXTRACTOR_dvi_extract_method function in plugins/dvi_extractor.c. **CVE ID : CVE-2017-15922**	NA	A-GNU-LIBEX-011117/24
Libextractor					
Overflow	18-10-2017	5	In GNU Libextractor 1.4, there is an integer signedness error for the chunk size in the EXTRACTOR_nsfe_extract_method function in plugins/nsfe_extractor.c, leading to an infinite loop for a crafted size. **CVE ID : CVE-2017-15602**	NA	A-GNU-LIBEX-011117/25
Overflow	18-10-2017	5	In GNU Libextractor 1.4, there is a heap-based buffer overflow in the EXTRACTOR_png_extract_method function in plugins/png_extractor.c, related to processiTXt and stndup. **CVE ID : CVE-2017-15601**	NA	A-GNU-LIBEX-011117/26
NA	18-10-2017	5	In GNU Libextractor 1.4, there is a NULL Pointer Dereference in the EXTRACTOR_nsf_extract_method function of plugins/nsf_extractor.c. **CVE ID : CVE-2017-15600**	NA	A-GNU-LIBEX-011117/27
Graphicsmagick					
Graphicsmagick					
NA	27-10-2017	6.8	In ReadOneJNGImage in coders/png.c in GraphicsMagick 1.3.26, a Null Pointer Dereference	https://sourceforge.net/p/g	A-GRA-GRAPH-011117/

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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
			occurs while transferring JPEG scanlines, related to a PixelPacket pointer. **CVE ID : CVE-2017-15930**	raphicsmagick/bugs/518/	28
IBM					
Bigfix Platform					
Gain Information	26-10-2017	4	IBM Tivoli Endpoint Manager (IBM BigFix Platform 9.2 and 9.5) generates an error message in error logs that includes sensitive information about its environment which could be used in further attacks against the system. IBM X-Force ID: 123905. **CVE ID : CVE-2017-1226**	http://www.ibm.com/support/docview.wss?uid=swg22009673	A-IBM-BIGFI-011117/29
XSS	26-10-2017	4.3	IBM Tivoli Endpoint Manager (for Lifecycle/Power/Patch) Platform and Applications (IBM BigFix Platform 9.2 and 9.5) is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 129831. **CVE ID : CVE-2017-1521**	http://www.ibm.com/support/docview.wss?uid=swg22009673	A-IBM-BIGFI-011117/30
Gain Information	26-10-2017	4.3	IBM Tivoli Endpoint Manager (IBM BigFix Platform 9.2 and 9.5) transmits sensitive or security-critical data in cleartext in a communication channel that can be sniffed by unauthorized actors. IBM X-Force ID: 123911. **CVE ID : CVE-2017-1232**	http://www.ibm.com/support/docview.wss?uid=swg22009673	A-IBM-BIGFI-011117/31
Gain Information	26-10-2017	4.3	IBM Tivoli Endpoint Manager (IBM BigFix Platform 9.2 and 9.5) could allow a remote attacker to obtain sensitive information, caused by the failure to properly enable the secure cookie attribute. An attacker could exploit this vulnerability to obtain sensitive information using man in the middle techniques. IBM X-Force	http://www.ibm.com/support/docview.wss?uid=swg22009673	A-IBM-BIGFI-011117/32

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ID: 123907. **CVE ID : CVE-2017-1228**		
Gain Information	26-10-2017	5	IBM Tivoli Endpoint Manager (IBM BigFix Platform 9.2 and 9.5) uses insufficiently random numbers or values in a security context that depends on unpredictable numbers. This weakness may allow attackers to expose sensitive information by guessing tokens or identifiers. IBM X-Force ID: 123909. **CVE ID : CVE-2017-1230**	http://www.ibm.com/support/docview.wss?uid=swg22009673	A-IBM-BIGFI-011117/33
Gain Information	26-10-2017	5	IBM Tivoli Endpoint Manager (IBM BigFix Platform 9.2 and 9.5) stores sensitive information in URL parameters. This may lead to information disclosure if unauthorized parties have access to the URLs via server logs, referrer header or browser history. IBM X-Force ID: 123904. **CVE ID : CVE-2017-1225**	http://www.ibm.com/support/docview.wss?uid=swg22009673	A-IBM-BIGFI-011117/34
Gain Information	26-10-2017	5	IBM Tivoli Endpoint Manager (IBM BigFix Platform 9.2 and 9.5) discloses sensitive information to unauthorized users. The information can be used to mount further attacks on the system. IBM X-Force ID: 123860. **CVE ID : CVE-2017-1220**	http://www.ibm.com/support/docview.wss?uid=swg22009673	A-IBM-BIGFI-011117/35
NA	26-10-2017	6.4	IBM Tivoli Endpoint Manager (IBM BigFix Platform 9.2 and 9.5) does not perform an authentication check for a critical resource or functionality allowing anonymous users access to protected areas. IBM X-Force ID: 123862. **CVE ID : CVE-2017-1222**	http://www.ibm.com/support/docview.wss?uid=swg22009673	A-IBM-BIGFI-011117/36
Daeja Viewone					
Gain Information	24-10-2017	1.9	IBM Daeja ViewONE Professional, Standard & Virtual 4.1.5.1 and 5.0.2 could disclose sensitive information to a local user when logging is enabled. IBM X-Force ID: 123851.	http://www.ibm.com/support/docview.wss?uid=swg22	A-IBM-DAEJA-011117/37

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2017-1211	008011	
XSS	24-10-2017	3.5	IBM Daeja ViewONE Professional, Standard & Virtual 4.1.5.1 and 5.0.2 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 123849. **CVE ID : CVE-2017-1209**	http://www.ibm.com/support/docview.wss?uid=swg22008010	A-IBM-DAEJA-011117/38
DoS	24-10-2017	4.3	IBM Daeja ViewONE Professional, Standard & Virtual 4.1.5.1 and 5.0.2 is vulnerable to a denial of service when viewing or opening a large file. IBM X-Force ID: 123852. **CVE ID : CVE-2017-1212**	http://www.ibm.com/support/docview.wss?uid=swg22007466	A-IBM-DAEJA-011117/39
NA	24-10-2017	5	IBM Daeja ViewONE Professional, Standard & Virtual 4.1.5.1 and 5.0.2 could allow an unauthenticated attacker to inject data into log files made to look legitimate. IBM X-Force ID: 123850. **CVE ID : CVE-2017-1210**	http://www.ibm.com/support/docview.wss?uid=swg22008009	A-IBM-DAEJA-011117/40
Irfanview					
Babacad4image;Irfanview					
DoS Overflow	22-10-2017	6.8	IrfanView 4.50 - 64bit with BabaCAD4Image plugin version 1.3 allows attackers to cause a denial of service or possibly have unspecified other impact via a crafted .dwg file, related to "Data from Faulting Address controls Branch Selection starting at BabaCAD4Image!ShowPlugInOptions+0x000000000001f0a0." **CVE ID : CVE-2017-15766**	https://github.com/wlinzi/security_advisories/tree/master/CVE-2017-15766	A-IRF-BABAC-011117/41
DoS Overflow	22-10-2017	6.8	IrfanView 4.50 - 64bit with BabaCAD4Image plugin version 1.3 allows attackers to cause a denial of service or possibly have unspecified other impact via a crafted .dwg file, related to a "Read	https://github.com/wlinzi/security_advisories/tree/ma	A-IRF-BABAC-011117/42

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Access Violation starting at BabaCAD4Image!ShowPlugInOptions+0x000000000001e6b0." **CVE ID : CVE-2017-15764**	ster/CVE-2017-15764	
DoS Execute Code Overflow	22-10-2017	6.8	IrfanView 4.50 - 64bit with BabaCAD4Image plugin version 1.3 allows attackers to Execute arbitrary code or cause a denial of service via a crafted .dwg file, related to "Data from Faulting Address controls subsequent Write Address starting at BabaCAD4Image!ShowPlugInOptions+0x000000000001eca0." **CVE ID : CVE-2017-15763**	https://github.com/wlinzi/security_advisories/tree/master/CVE-2017-15763	A-IRF-BABAC-011117/43
DoS Execute Code Overflow	22-10-2017	6.8	IrfanView 4.50 - 64bit with BabaCAD4Image plugin version 1.3 allows attackers to Execute arbitrary code or cause a denial of service via a crafted .dwg file, related to a "User Mode Write AV near NULL starting at BabaCAD4Image!ShowPlugInOptions+0x000000000001f31b." **CVE ID : CVE-2017-15762**	https://github.com/wlinzi/security_advisories/tree/master/CVE-2017-15762	A-IRF-BABAC-011117/44
DoS Execute Code Overflow	22-10-2017	6.8	IrfanView 4.50 - 64bit with BabaCAD4Image plugin version 1.3 allows attackers to Execute arbitrary code or cause a denial of service via a crafted .dwg file, related to a "User Mode Write AV starting at BabaCAD4Image!ShowPlugInOptions+0x000000000001ecaa." **CVE ID : CVE-2017-15761**	https://github.com/wlinzi/security_advisories/tree/master/CVE-2017-15761	A-IRF-BABAC-011117/45
DoS Execute Code Overflow	22-10-2017	6.8	IrfanView 4.50 - 64bit with BabaCAD4Image plugin version 1.3 allows attackers to Execute arbitrary code or cause a denial of service via a crafted .dwg file, related to a "User Mode Write AV near NULL starting at BabaCAD4Image!ShowPlugInOptions+0x000000000001ce82." **CVE ID : CVE-2017-15760**	https://github.com/wlinzi/security_advisories/tree/master/CVE-2017-15760	A-IRF-BABAC-011117/46
DoS Execute	22-10-2017	6.8	IrfanView 4.50 - 64bit with	https://gi	A-IRF-

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Code Overflow			BabaCAD4Image plugin version 1.3 allows attackers to Execute arbitrary code or cause a denial of service via a crafted .dwg file, related to a "User Mode Write AV near NULL starting at BabaCAD4Image!ShowPlugInOptions+0x000000000001b3f3." **CVE ID : CVE-2017-15759**	thub.com /wlinzi/security_advisories /tree/master/CVE-2017-15759	BABAC-011117/47
DoS Execute Code Overflow	22-10-2017	6.8	IrfanView 4.50 - 64bit with BabaCAD4Image plugin version 1.3 allows attackers to Execute arbitrary code or cause a denial of service via a crafted .dwg file, related to "Data from Faulting Address controls subsequent Write Address starting at BabaCAD4Image!ShowPlugInOptions+0x000000000004d75b." **CVE ID : CVE-2017-15758**	https://github.com /wlinzi/security_advisories /tree/master/CVE-2017-15758	A-IRF-BABAC-011117/48
DoS Overflow	22-10-2017	6.8	IrfanView 4.50 - 64bit with BabaCAD4Image plugin version 1.3 allows attackers to cause a denial of service or possibly have unspecified other impact via a crafted .dwg file, related to "Data from Faulting Address controls Branch Selection starting at BabaCAD4Image!ShowPlugInOptions+0x00000000000029ba." **CVE ID : CVE-2017-15757**	https://github.com /wlinzi/security_advisories /tree/master/CVE-2017-15757	A-IRF-BABAC-011117/49
DoS Execute Code Overflow	22-10-2017	6.8	IrfanView 4.50 - 64bit with BabaCAD4Image plugin version 1.3 allows attackers to Execute arbitrary code or cause a denial of service via a crafted .dwg file, related to "Data from Faulting Address controls subsequent Write Address starting at BabaCAD4Image!ShowPlugInOptions+0x000000000004d7c4." **CVE ID : CVE-2017-15756**	https://github.com /wlinzi/security_advisories /tree/master/CVE-2017-15756	A-IRF-BABAC-011117/50
DoS Overflow	22-10-2017	6.8	IrfanView 4.50 - 64bit with BabaCAD4Image plugin version 1.3 allows attackers to cause a denial of service or possibly have	https://github.com /wlinzi/security_a	A-IRF-BABAC-011117/51

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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
			unspecified other impact via a crafted .dwg file, related to "Data from Faulting Address controls Branch Selection starting at verifier!AVrfpDphFindBusyMemoryNoCheck+0x0000000000000091." **CVE ID : CVE-2017-15755**	dvisories /tree/master/CVE-2017-15755	
DoS Execute Code Overflow	22-10-2017	6.8	IrfanView 4.50 - 64bit with BabaCAD4Image plugin version 1.3 allows attackers to Execute arbitrary code or cause a denial of service via a crafted .dwg file, related to a "User Mode Write AV near NULL starting at BabaCAD4Image!ShowPlugInOptions+0x0000000000013968." **CVE ID : CVE-2017-15754**	https://github.com/wlinzi/security_advisories/tree/master/CVE-2017-15754	A-IRF-BABAC-011117/52
DoS Overflow	22-10-2017	6.8	IrfanView 4.50 - 64bit with BabaCAD4Image plugin version 1.3 allows attackers to cause a denial of service or possibly have unspecified other impact via a crafted .dwg file, related to "Data from Faulting Address controls Branch Selection starting at BabaCAD4Image!ShowPlugInOptions+0x00000000029c2." **CVE ID : CVE-2017-15753**	https://github.com/wlinzi/security_advisories/tree/master/CVE-2017-15753	A-IRF-BABAC-011117/53
DoS Execute Code Overflow	22-10-2017	6.8	IrfanView 4.50 - 64bit with BabaCAD4Image plugin version 1.3 allows attackers to Execute arbitrary code or cause a denial of service via a crafted .dwg file, related to "Data from Faulting Address controls subsequent Write Address starting at BabaCAD4Image!ShowPlugInOptions+0x000000000004d6b0." **CVE ID : CVE-2017-15752**	https://github.com/wlinzi/security_advisories/tree/master/CVE-2017-15752	A-IRF-BABAC-011117/54
DoS Overflow	22-10-2017	6.8	IrfanView 4.50 - 64bit with BabaCAD4Image plugin version 1.3 allows attackers to cause a denial of service or possibly have unspecified other impact via a crafted .dwg file, related to a "Read Access Violation starting at	https://github.com/wlinzi/security_advisories/tree/master/CVE-	A-IRF-BABAC-011117/55

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			BabaCAD4Image!ShowPlugInOptions+0x0000000000009f39." **CVE ID : CVE-2017-15751**	2017-15751	
DoS Overflow	22-10-2017	6.8	IrfanView 4.50 - 64bit with BabaCAD4Image plugin version 1.3 allows attackers to cause a denial of service or possibly have unspecified other impact via a crafted .dwg file, related to a "Read Access Violation starting at BabaCAD4Image!ShowPlugInOptions+0x0000000000009ae0." **CVE ID : CVE-2017-15750**	https://github.com/wlinzi/security_advisories/tree/master/CVE-2017-15750	A-IRF-BABAC-011117/56
Cadimage;Irfanview					
DoS Execute Code Overflow	22-10-2017	6.8	IrfanView 4.50 - 64bit with CADImage plugin version 12.0.0.5 allows attackers to Execute arbitrary code or cause a denial of service via a crafted .dwg file, related to a "User Mode Write AV near NULL starting at CADIMAGE+0x00000000003d5b52."**CVE ID : CVE-2017-15767**	https://github.com/wlinzi/security_advisories/tree/master/CVE-2017-15767	A-IRF-CADIM-011117/57
DoS Overflow	22-10-2017	6.8	IrfanView 4.50 - 64bit with CADImage plugin version 12.0.0.5 allows attackers to cause a denial of service or possibly have unspecified other impact via a crafted .dwg file, related to "Data from Faulting Address is used as one or more arguments in a subsequent Function Call starting at CADIMAGE+0x00000000003e9462." **CVE ID : CVE-2017-15765**	https://github.com/wlinzi/security_advisories/tree/master/CVE-2017-15765	A-IRF-CADIM-011117/58
DoS Overflow	22-10-2017	6.8	IrfanView 4.50 - 64bit with CADImage plugin version 12.0.0.5 allows attackers to cause a denial of service or possibly have unspecified other impact via a crafted .dwg file, related to "Data from Faulting Address controls Branch Selection starting at CADIMAGE+0x00000000000348b9." **CVE ID : CVE-2017-15749**	https://github.com/wlinzi/security_advisories/tree/master/CVE-2017-15749	A-IRF-CADIM-011117/59
DoS Execute	22-10-2017	6.8	IrfanView 4.50 - 64bit with	https://gi	A-IRF-

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Code Overflow			CADImage plugin version 12.0.0.5 allows attackers to Execute arbitrary code or cause a denial of service via a crafted .dwg file, related to a "User Mode Write AV starting at CADIMAGE+0x000000000000613a." **CVE ID : CVE-2017-15748**	thub.com /wlinzi/security_advisories /tree/master/CVE-2017-15748	CADIM-011117/60
DoS Execute Code Overflow	22-10-2017	6.8	IrfanView 4.50 - 64bit with CADImage plugin version 12.0.0.5 allows attackers to Execute arbitrary code or cause a denial of service via a crafted .dwg file, related to a "Data Executeution Prevention Violation starting at Unknown Symbol @ 0x0000700b00260112 called from CADIMAGE+0x00000000003d35ad." **CVE ID : CVE-2017-15747**	https://github.com /wlinzi/security_advisories /tree/master/CVE-2017-15747	A-IRF-CADIM-011117/61
DoS Overflow	22-10-2017	6.8	IrfanView 4.50 - 64bit with CADImage plugin version 12.0.0.5 allows attackers to cause a denial of service or possibly have unspecified other impact via a crafted .dwg file, related to "Data from Faulting Address controls Branch Selection starting at CADIMAGE+0x00000000003d21b3." **CVE ID : CVE-2017-15746**	https://github.com /wlinzi/security_advisories /tree/master/CVE-2017-15746	A-IRF-CADIM-011117/62
DoS Overflow	22-10-2017	6.8	IrfanView 4.50 - 64bit with CADImage plugin version 12.0.0.5 allows attackers to cause a denial of service or possibly have unspecified other impact via a crafted .dwg file, related to "Data from Faulting Address controls Branch Selection starting at CADIMAGE+0x000000000002ca2e." **CVE ID : CVE-2017-15745**	https://github.com /wlinzi/security_advisories /tree/master/CVE-2017-15745	A-IRF-CADIM-011117/63
DoS Execute Code Overflow	22-10-2017	6.8	IrfanView 4.50 - 64bit with CADImage plugin version 12.0.0.5 allows attackers to Execute arbitrary code or cause a denial of service via a crafted .dwg file, related to a "Read Access Violation on Control Flow starting at	https://github.com /wlinzi/security_advisories /tree/master/CVE-	A-IRF-CADIM-011117/64

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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
			CADIMAGE+0x00000000003d35a7." **CVE ID : CVE-2017-15744**	2017-15744	
DoS Overflow	22-10-2017	6.8	IrfanView 4.50 - 64bit with CADImage plugin version 12.0.0.5 allows attackers to cause a denial of service or possibly have unspecified other impact via a crafted .dwg file, related to "Data from Faulting Address may be used as a return value starting at CADIMAGE+0x00000000003d24a0." **CVE ID : CVE-2017-15743**	https://github.com/wlinzi/security_advisories/tree/master/CVE-2017-15743	A-IRF-CADIM-011117/65
DoS Overflow	22-10-2017	6.8	IrfanView 4.50 - 64bit with CADImage plugin version 12.0.0.5 allows attackers to cause a denial of service or possibly have unspecified other impact via a crafted .dwg file, related to a "Read Access Violation starting at CADIMAGE+0x00000000003d2328." **CVE ID : CVE-2017-15742**	https://github.com/wlinzi/security_advisories/tree/master/CVE-2017-15742	A-IRF-CADIM-011117/66
DoS Overflow	22-10-2017	6.8	IrfanView 4.50 - 64bit with CADImage plugin version 12.0.0.5 allows attackers to cause a denial of service or possibly have unspecified other impact via a crafted .dwg file, related to "Possible Stack Corruption starting at CADIMAGE+0x00000000003d2378." **CVE ID : CVE-2017-15741**	https://github.com/wlinzi/security_advisories/tree/master/CVE-2017-15741	A-IRF-CADIM-011117/67
DoS Execute Code Overflow	22-10-2017	6.8	IrfanView 4.50 - 64bit with CADImage plugin version 12.0.0.5 allows attackers to Execute arbitrary code or cause a denial of service via a crafted .dwg file, related to "Data from Faulting Address controls Code Flow starting at CADIMAGE+0x000000000033228e." **CVE ID : CVE-2017-15740**	https://github.com/wlinzi/security_advisories/tree/master/CVE-2017-15740	A-IRF-CADIM-011117/68
DoS Execute Code Overflow	22-10-2017	6.8	IrfanView 4.50 - 64bit with CADImage plugin version 12.0.0.5 allows attackers to Execute arbitrary code or cause a denial of service via a crafted .dwg file,	https://github.com/wlinzi/security_advisories	A-IRF-CADIM-011117/69

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			related to "Data from Faulting Address controls subsequent Write Address starting at CADIMAGE+0x00000000000042d5." **CVE ID : CVE-2017-15739**	/tree/master/CVE-2017-15739	
DoS Overflow	22-10-2017	6.8	IrfanView 4.50 - 64bit with CADImage plugin version 12.0.0.5 allows attackers to cause a denial of service or possibly have unspecified other impact via a crafted .dwg file, related to a "Read Access Violation starting at CADIMAGE+0x00000000003d22d8." **CVE ID : CVE-2017-15738**	https://github.com/wlinzi/security_advisories/tree/master/CVE-2017-15738	A-IRF-CADIM-011117/70
DoS Overflow	22-10-2017	6.8	IrfanView 4.50 - 64bit with CADImage plugin version 12.0.0.5 allows attackers to cause a denial of service or possibly have unspecified other impact via a crafted .dwg file, related to a "Read Access Violation starting at CADIMAGE+0x00000000003d246f." **CVE ID : CVE-2017-15737**	https://github.com/wlinzi/security_advisories/tree/master/CVE-2017-15737	A-IRF-CADIM-011117/71
Irfanview					
DoS Execute Code Overflow	22-10-2017	6.8	IrfanView version 4.50 (64bit) allows attackers to Execute arbitrary code or cause a denial of service via a crafted .dll file that is mishandled during an attempt to render the DLL icon, related to "Data from Faulting Address controls subsequent Write Address starting at ntdll!memcpy+0x00000000000000a0." **CVE ID : CVE-2017-15800**	https://github.com/wlinzi/security_advisories/tree/master/CVE-2017-15800	A-IRF-IRFAN-011117/72
DoS Overflow	22-10-2017	6.8	IrfanView version 4.50 (64bit) allows attackers to cause a denial of service or possibly have unspecified other impact via a crafted .dll file that is mishandled during an attempt to render the DLL icon, related to "Data from Faulting Address controls Branch Selection starting at KERNELBASE!EnumResourceNamesInternal+0x000000000000074a	https://github.com/wlinzi/security_advisories/tree/master/CVE-2017-15799	A-IRF-IRFAN-011117/73

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2017-15799**		
DoS Overflow	22-10-2017	6.8	IrfanView version 4.50 (64bit) allows attackers to cause a denial of service or possibly have unspecified other impact via a crafted .dll file that is mishandled during an attempt to render the DLL icon, related to "Data from Faulting Address controls Branch Selection starting at KERNELBASE!EnumResourceNamesInternal+0x0000000000000609."**CVE ID : CVE-2017-15798**	https://github.com/wlinzi/security_advisories/tree/master/CVE-2017-15798	A-IRF-IRFAN-011117/74
DoS Execute Code Overflow	22-10-2017	6.8	IrfanView version 4.50 (64bit) allows attackers to Execute arbitrary code or cause a denial of service via a crafted .dll file that is mishandled during an attempt to render the DLL icon, related to a "Read Access Violation on Block Data Move starting at TOOLS!IVLoadImage_W+0x0000000000000020b9." **CVE ID : CVE-2017-15797**	https://github.com/wlinzi/security_advisories/tree/master/CVE-2017-15797	A-IRF-IRFAN-011117/75
DoS Overflow	22-10-2017	6.8	IrfanView version 4.50 (64bit) allows attackers to cause a denial of service or possibly have unspecified other impact via a crafted .dll file that is mishandled during an attempt to render the DLL icon, related to a "Read Access Violation starting at ntdll!LdrpSearchResourceSection_U+0x0000000000000386." **CVE ID : CVE-2017-15796**	https://github.com/wlinzi/security_advisories/tree/master/CVE-2017-15796	A-IRF-IRFAN-011117/76
DoS Overflow	22-10-2017	6.8	IrfanView version 4.50 (64bit) allows attackers to cause a denial of service or possibly have unspecified other impact via a crafted .dll file that is mishandled during an attempt to render the DLL icon, related to a "Read Access Violation starting at ntdll!LdrpSearchResourceSection_U+0x00000000000002bd." **CVE ID : CVE-2017-15795**	https://github.com/wlinzi/security_advisories/tree/master/CVE ID :CVE-2017-15795	A-IRF-IRFAN-011117/77

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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
DoS Overflow	22-10-2017	6.8	IrfanView version 4.50 (64bit) allows attackers to cause a denial of service or possibly have unspecified other impact via a crafted .dll file that is mishandled during an attempt to render the DLL icon, related to a "Read Access Violation starting at ntdll!LdrpResSearchResourceInsideDirectory+0x0000000000000257." **CVE ID : CVE-2017-15794**	https://github.com/wlinzi/security_advisories/tree/master/CVE-2017-15794	A-IRF-IRFAN-011117/78
DoS Execute Code Overflow	22-10-2017	6.8	IrfanView version 4.50 (64bit) allows attackers to Execute arbitrary code or cause a denial of service via a crafted .dll file that is mishandled during an attempt to render the DLL icon, related to "Data from Faulting Address controls subsequent Write Address starting at ntdll!memcpy+0x00000000000000a5." **CVE ID : CVE-2017-15793**	https://github.com/wlinzi/security_advisories/tree/master/CVE-2017-15793	A-IRF-IRFAN-011117/79
DoS Overflow	22-10-2017	6.8	IrfanView version 4.50 (64bit) allows attackers to cause a denial of service or possibly have unspecified other impact via a crafted .dll file that is mishandled during an attempt to render the DLL icon, related to "Data from Faulting Address controls Branch Selection starting at KERNELBASE!EnumResourceTypesInternal+0x00000000000007b2." **CVE ID : CVE-2017-15792**	https://github.com/wlinzi/security_advisories/tree/master/CVE-2017-15792	A-IRF-IRFAN-011117/80
DoS Overflow	22-10-2017	6.8	IrfanView version 4.50 (64bit) allows attackers to cause a denial of service or possibly have unspecified other impact via a crafted .dll file that is mishandled during an attempt to render the DLL icon, related to "Data from Faulting Address controls Branch Selection starting at ntdll!LdrpResCompareResourceNames+0x00000000000000de." **CVE ID : CVE-2017-15791**	https://github.com/wlinzi/security_advisories/tree/master/CVE-2017-15791	A-IRF-IRFAN-011117/81

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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
DoS Overflow	22-10-2017	6.8	IrfanView version 4.50 (64bit) allows attackers to cause a denial of service or possibly have unspecified other impact via a crafted .dll file that is mishandled during an attempt to render the DLL icon, related to a "Read Access Violation starting at ntdll!LdrpResCompareResourceNames+0x0000000000000120." **CVE ID : CVE-2017-15790**	https://github.com/wlinzi/security_advisories/tree/master/CVE-2017-15790	A-IRF-IRFAN-011117/82
DoS Overflow	22-10-2017	6.8	IrfanView 4.50 - 64bit allows attackers to cause a denial of service or possibly have unspecified other impact via a crafted .dds file, related to "Read Access Violation starting at FORMATS!ReadBLP_W+0x0000000000001b22." **CVE ID : CVE-2017-15769**	https://github.com/wlinzi/security_advisories/tree/master/CVE-2017-15769	A-IRF-IRFAN-011117/83
DoS Overflow	22-10-2017	6.8	IrfanView version 4.50 - 64bit allows attackers to cause a denial of service or possibly have unspecified other impact via a crafted .tif file, related to "Data from Faulting Address controls Branch Selection starting at image000007f7_42060000+0x0000000000094113." **CVE ID : CVE-2017-15768**	https://github.com/wlinzi/security_advisories/tree/master/CVE-2017-15768	A-IRF-IRFAN-011117/84
Irssi					
Irssi					
NA	22-10-2017	5	In Irssi before 1.0.5, overlong nicks or targets may result in a NULL pointer dereference while splitting the message. **CVE ID : CVE-2017-15723**	https://irssi.org/security/irssi_sa_2017_10.txt	A-IRS-IRSSI-011117/85
NA	22-10-2017	5	In certain cases, Irssi before 1.0.5 may fail to verify that a Safe channel ID is long enough, causing reads beyond the end of the string. **CVE ID : CVE-2017-15722**	https://irssi.org/security/irssi_sa_2017_10.txt	A-IRS-IRSSI-011117/86
NA	22-10-2017	5	In Irssi before 1.0.5, certain incorrectly formatted DCC CTCP messages could cause a NULL pointer dereference. This is a	http://openwall.com/lists/oss-	A-IRS-IRSSI-011117/87

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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
			separate, but similar, issue relative to CVE ID :CVE-2017-9468. **CVE ID : CVE-2017-15721**	security/2017/10/22/4	
NA	22-10-2017	5	Irssi before 1.0.5, when installing themes with unterminated colour formatting sequences, may access data beyond the end of the string. **CVE ID : CVE-2017-15228**	https://irssi.org/security/irssi_sa_2017_10.txt	A-IRS-IRSSI-011117/88
NA	22-10-2017	5	Irssi before 1.0.5, while waiting for the channel synchronisation, may incorrectly fail to remove destroyed channels from the query list, resulting in use-after-free conditions when updating the state later on. **CVE ID : CVE-2017-15227**	https://irssi.org/security/irssi_sa_2017_10.txt	A-IRS-IRSSI-011117/89
Labwiki Project					
Labwiki					
XSS	23-10-2017	4.3	Multiple cross-site scripting (XSS) vulnerabilities in LabWiki 1.1 and earlier allow remote attackers to inject arbitrary web script or HTML via the (1) from parameter to index.php or the (2) page_no parameter to recentchanges.php. **CVE ID : CVE-2011-4333**	NA	A-LAB-LABWI-011117/90
Labwiki					
NA	23-10-2017	6.5	edit.php in LabWiki 1.1 and earlier does not properly verify uploaded user files, which allows remote authenticated users to upload arbitrary PHP files via a PHP file with a .gif extension in the userfile parameter. **CVE ID : CVE-2011-4334**	NA	A-LAB-LABWI-011117/91
Mediawiki					
Mediawiki					
Gain Information	19-10-2017	4	MediaWiki before 1.18.5, and 1.19.x before 1.19.2 does not properly protect user block metadata, which allows remote administrators to read a user block reason via a reblock attempt. **CVE ID : CVE-2012-4382**	https://phabricator.wikimedia.org/T41823	A-MED-MEDIA-011117/92
NA	19-10-2017	4.3	MediaWiki before 1.18.5, and	https://p	A-MED-

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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
			1.19.x before 1.19.2 does not send a restrictive X-Frame-Options HTTP header, which allows remote attackers to conduct clickjacking attacks via an embedded API response in an IFRAME element. **CVE ID : CVE-2012-4379**	habricator.wikimedia.org/T41180	MEDIA-011117/93
XSS	26-10-2017	4.3	Multiple cross-site scripting (XSS) vulnerabilities in MediaWiki before 1.18.5 and 1.19.x before 1.19.2, when unspecified JavaScript gadgets are used, allow remote attackers to inject arbitrary web script or HTML via the userlang parameter to w/index.php. **CVE ID : CVE-2012-4378**	https://phabricator.wikimedia.org/T39587	A-MED-MEDIA-011117/94
XSS	26-10-2017	4.3	Cross-site scripting (XSS) vulnerability in MediaWiki before 1.18.5 and 1.19.x before 1.19.2 allows remote attackers to inject arbitrary web script or HTML via a File: link to a nonexistent image. **CVE ID : CVE-2012-4377**	https://bugzilla.redhat.com/show_bug.cgi?id=853409	A-MED-MEDIA-011117/95
Bypass	19-10-2017	5	MediaWiki before 1.18.5, and 1.19.x before 1.19.2 allows remote attackers to bypass GlobalBlocking extension IP address blocking and create an account via unspecified vectors. **CVE ID : CVE-2012-4380**	https://phabricator.wikimedia.org/T41824	A-MED-MEDIA-011117/96
Octopus					
Octopus Deploy					
NA	19-10-2017	4	In Octopus before 3.17.7, an authenticated user who was explicitly granted the permission to invite new users (aka UserInvite) can invite users to teams with escalated privileges. **CVE ID : CVE-2017-15611**	https://github.com/OctopusDeploy/Issues/issues/3864	A-OCT-OCTOP-011117/97
Gain Information	19-10-2017	4	An issue was discovered in Octopus before 3.17.7. When the special Guest user account is granted the CertificateExportPrivateKey	https://github.com/OctopusDeploy/Issues/issu	A-OCT-OCTOP-011117/98

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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
			permission, and Guest Access is enabled for the Octopus Server, an attacker can sign in as the Guest account and export Certificates managed by Octopus, including the private key. **CVE ID : CVE-2017-15610**	es/3869	
Gain Information	19-10-2017	5	Octopus before 3.17.7 allows attackers to obtain sensitive cleartext information by reading a variable JSON file in certain situations involving Offline Drop Targets. **CVE ID : CVE-2017-15609**	https://github.com/OctopusDeploy/Issues/issues/3868	A-OCT-OCTOP-011117/99
Oracle					
Access Manager					
Gain Information	19-10-2017	5	Vulnerability in the Oracle Access Manager component of Oracle Fusion Middleware (subcomponent: Web Server Plugin). The supported version that is affected is 11.1.2.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Access Manager. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Access Manager 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-2017-10154**	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-ACCES-011117/100
Advanced Outbound Telephony					
NA	19-10-2017	5.8	Vulnerability in the Oracle Advanced Outbound Telephony component of Oracle E-Business Suite (subcomponent: Setup and Configuration). Supported versions that are affected are 12.2.3, 12.2.4, 12.2.5, 12.2.6 and 12.2.7. Easily exploitable vulnerability allows	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.	A-ORA-ADVAN-011117/101

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated attacker with network access via HTTP to compromise Oracle Advanced Outbound Telephony. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Advanced Outbound Telephony, 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 Advanced Outbound Telephony accessible data as well as unauthorized update, insert or delete access to some of Oracle Advanced Outbound Telephony 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-2017-10417**	html	
NA	19-10-2017	5.8	Vulnerability in the Oracle Advanced Outbound Telephony component of Oracle E-Business Suite (subcomponent: Setup and Configuration). Supported versions that are affected are 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 Advanced Outbound Telephony. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Advanced Outbound Telephony, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-ADVAN-011117/102

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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
			unauthorized access to critical data or complete access to all Oracle Advanced Outbound Telephony accessible data as well as unauthorized update, insert or delete access to some of Oracle Advanced Outbound Telephony 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-2017-10416**		
Agile Engineering Data Management					
NA	19-10-2017	5.8	Vulnerability in the Oracle Engineering Data Management component of Oracle Supply Chain Products Suite (subcomponent: Web Services Security). Supported versions that are affected are 6.1.3.0 and 6.2.2.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Engineering Data Management. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Engineering Data Management accessible data as well as unauthorized read access to a subset of Oracle Engineering Data Management 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-2017-10161**	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-AGILE-011117/103
Agile Product Lifecycle Management Framework					
NA	19-10-2017	3.6	Vulnerability in the Oracle Agile PLM component of Oracle Supply Chain Products Suite (subcomponent: Performance). Supported versions that are	http://www.oracle.com/technetwork/security-	A-ORA-AGILE-011117/104

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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
			affected are 9.3.5 and 9.3.6. Easily exploitable vulnerability allows physical access to compromise Oracle Agile PLM. 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 3.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:P/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N). **CVE ID : CVE-2017-10308**	advisory/cpuoct2017-3236626.html	
Gain Information	19-10-2017	4	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 low privileged attacker with network access via HTTP to compromise Oracle Agile PLM. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Agile PLM 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-2017-10299**	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-AGILE-011117/105
Application Object Library					
Gain Information	19-10-2017	5	Vulnerability in the Oracle Application Object Library component of Oracle E-Business Suite (subcomponent: Diagnostics). Supported versions that are affected are 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6 and 12.2.7. Easily exploitable vulnerability allows unauthenticated attacker	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.	A-ORA-APPLI-011117/106

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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
			with network access via HTTP to compromise Oracle Application Object Library. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Application Object Library 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-2017-10331**	html	
Gain Information	19-10-2017	5	Vulnerability in the Oracle Application Object Library component of Oracle E-Business Suite (subcomponent: Diagnostics). Supported versions that are affected are 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6 and 12.2.7. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Application Object Library. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Application Object Library 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-2017-10328**	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-APPLI-011117/107
Applications Dba					
NA	19-10-2017	5.5	Vulnerability in the Oracle Applications DBA component of Oracle E-Business Suite (subcomponent: AD Utilities). 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 Applications	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-APPLI-011117/108

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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
			DBA. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Applications DBA accessible data as well as unauthorized access to critical data or complete access to all Oracle Applications DBA accessible data. CVSS 3.0 Base Score 6.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:N). **CVE ID : CVE-2017-10077**		
Business Intelligence					
NA	19-10-2017	4.9	Vulnerability in the Oracle Business Intelligence Enterprise Edition component of Oracle Fusion Middleware (subcomponent: Analytics Web General). Supported versions that are affected are 11.1.1.7.0, 11.1.1.9.0, 12.2.1.1.0 and 12.2.1.2.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Business Intelligence Enterprise Edition accessible data as well as unauthorized read access to a subset of Oracle Business Intelligence Enterprise Edition accessible data. Note: Please refer to Doc ID <a href="http://support.oracle.com/CSP/main/article?cmd=show&type=NOT&id=2310021.1">My Oracle	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-BUSIN-011117/109

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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
			Support Note 2310021.1 for instructions on how to address this issue. CVSS 3.0 Base Score 6.3 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:H/A:N). **CVE ID : CVE-2017-10163**		
NA	19-10-2017	5.8	Vulnerability in the Oracle Business Intelligence Enterprise Edition component of Oracle Fusion Middleware (subcomponent: Analytics Web General). Supported versions that are affected are 11.1.1.7.0, 11.1.1.9.0, 12.2.1.1.0 and 12.2.1.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network 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-2017-10060**	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-BUSIN-011117/110
Business Intelligence Publisher					
Gain	19-10-2017	5	Vulnerability in the Oracle BI	http://w	A-ORA-

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information			Publisher component of Oracle Fusion Middleware (subcomponent: Web Service API). Supported versions that are affected are 11.1.1.7.0 and 11.1.1.9.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle BI Publisher. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle BI Publisher 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-2017-10037**	ww.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	BUSIN-011117/111
NA	19-10-2017	5.8	Vulnerability in the Oracle BI Publisher component of Oracle Fusion Middleware (subcomponent: Core Formatting API). Supported versions that are affected are 11.1.1.7.0 and 11.1.1.9.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle BI Publisher. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle BI Publisher, 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 BI Publisher accessible data as well as unauthorized update, insert or delete access to some of Oracle BI Publisher accessible	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-BUSIN-011117/112

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2017-10034**		
Common Applications					
NA	19-10-2017	6.4	Vulnerability in the Oracle Common Applications component of Oracle E-Business Suite (subcomponent: Gantt Server). Supported versions that are affected are 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6 and 12.2.7. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Common Applications. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Common Applications accessible data as well as unauthorized access to critical data or complete access to all Oracle Common Applications 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-2017-10330**	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-COMMO-011117/113
Common Applications Calendar					
NA	19-10-2017	5	Vulnerability in the Oracle Common Applications Calendar component of Oracle E-Business Suite (subcomponent: Applications Calendar). 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 Common	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-COMMO-011117/114

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Applications Calendar. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Common Applications Calendar accessible data. CVSS 3.0 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2017-10322**		
NA	19-10-2017	5.8	Vulnerability in the Oracle Common Applications Calendar component of Oracle E-Business Suite (subcomponent: Applications Calendar). 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 Common Applications Calendar. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Common Applications Calendar, 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 Common Applications Calendar accessible data as well as unauthorized update, insert or delete access to some of Oracle Common Applications Calendar 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-2017-10326**	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-COMMO-011117/115
NA	19-10-2017	5.8	Vulnerability in the Oracle	http://w	A-ORA-

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Common Applications Calendar component of Oracle E-Business Suite (subcomponent: Applications Calendar). 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 Common Applications Calendar. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Common Applications Calendar, 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 Common Applications Calendar accessible data as well as unauthorized update, insert or delete access to some of Oracle Common Applications Calendar 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-2017-10325**	ww.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	COMMO-011117/116
Communications Policy Management					
NA	19-10-2017	5.8	Vulnerability in the Oracle Communications Policy Management component of Oracle Communications Applications (subcomponent: Portal, CMP). Supported versions that are affected are 11.5 and 12.x. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Communications Policy	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-COMMU-011117/117

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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
			Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Communications Policy 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 Communications Policy Management accessible data as well as unauthorized read access to a subset of Oracle Communications Policy 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-2017-10159**		
Communications Webrtc Session Controller					
NA	19-10-2017	3.5	Vulnerability in the Oracle Communications WebRTC Session Controller component of Oracle Communications Applications (subcomponent: Security (Gson)). Supported versions that are affected are 7.0, 7.1 and 7.2. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise Oracle Communications WebRTC Session Controller. While the vulnerability is in Oracle Communications WebRTC Session Controller, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Communications	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-COMMU-011117/118

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			WebRTC Session Controller. CVSS 3.0 Base Score 6.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:N/I:N/A:H). **CVE ID : CVE-2017-10153**		
Coreid Access					
Gain Information	19-10-2017	5	Vulnerability in the Oracle Access Manager component of Oracle Fusion Middleware (subcomponent: Web Server Plugin). The supported version that is affected is 11.1.2.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP 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 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-2017-10259**	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-COREI-011117/119
Customer Relationship Management Technical Foundation					
NA	19-10-2017	4.3	Vulnerability in the Oracle CRM Technical Foundation component of Oracle E-Business Suite (subcomponent: Preferences). Supported versions that are affected are 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6 and 12.2.7. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle CRM Technical Foundation. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-CUSTO-011117/120

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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
			delete access to some of Oracle CRM Technical Foundation accessible data. CVSS 3.0 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N). **CVE ID : CVE-2017-10387**		
Database					
NA	19-10-2017	1.7	Vulnerability in the RDBMS Security component of Oracle Database Server. Supported versions that are affected are 11.2.0.4, 12.1.0.2 and 12.2.0.1. Easily exploitable vulnerability allows high privileged attacker having Create User privilege with logon to the infrastructure where RDBMS Security Executeutes to compromise RDBMS Security. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of RDBMS Security accessible data. CVSS 3.0 Base Score 2.3 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2017-10292**	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-DATAB-011117/121
Gain Information	19-10-2017	4	Vulnerability in the XML Database component of Oracle Database Server. Supported versions that are affected are 11.2.0.4 and 12.1.0.2. Easily exploitable vulnerability allows low privileged attacker having Create Session privilege with logon to the infrastructure where XML Database Executeutes to compromise XML Database. While the vulnerability is in XML Database, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-DATAB-011117/122

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthorized access to critical data or complete access to all XML Database accessible data. Note: This score is for Windows platform version 11.2.0.4 of Database. For Windows platform version 12.1.0.2 and Linux, the score is 5.5 with scope Unchanged. CVSS 3.0 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N). **CVE ID : CVE-2017-10261**		
NA	19-10-2017	4.3	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. Easily exploitable vulnerability allows high privileged attacker having Create Session, Create Procedure privilege with logon to the infrastructure where Java VM Executeutes to compromise Java VM. 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 8.2 (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-2017-10190**	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-DATAB-011117/123
NA	19-10-2017	4.6	Vulnerability in the Core RDBMS component of Oracle Database Server. Supported versions that are affected are 11.2.0.4, 12.1.0.2 and 12.2.0.1. Easily exploitable vulnerability allows low privileged attacker having Create session privilege with logon to the infrastructure where Core RDBMS	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.	A-ORA-DATAB-011117/124

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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
			Executeutes 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. Note: This score is for Windows platform version 11.2.0.4 of Database. For Windows platform version 12.1.0.2 and Linux, the score is 7.8 with scope Unchanged. 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-2017-10321**	html	
E-business Suite Technology Stack					
Gain Information	19-10-2017	5	Vulnerability in the Oracle Applications Technology Stack component of Oracle E-Business Suite (subcomponent: Oracle Forms). Supported versions that are affected are 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6 and 12.2.7. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Applications Technology Stack. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Applications Technology Stack 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-2017-10324**	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-E-BUS-011117/125
NA	19-10-2017	5	Vulnerability in the Oracle Applications Technology Stack component of Oracle E-Business Suite (subcomponent: Oracle Forms). Supported versions that	http://www.oracle.com/technetwork/security-	A-ORA-E-BUS-011117/126

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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
			are affected are 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6 and 12.2.7. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Applications Technology Stack. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Applications Technology Stack accessible data. CVSS 3.0 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2017-10066**	advisory/cpuoct2017-3236626.html	
Flexcube Universal Banking					
NA	19-10-2017	5.5	Vulnerability in the Oracle FLEXCUBE Universal Banking component of Oracle Financial Services Applications (subcomponent: Security). Supported versions that are affected are 11.3, 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 access to critical data or complete access to all Oracle FLEXCUBE Universal Banking accessible data as well as unauthorized update, insert or delete access to some of Oracle FLEXCUBE Universal Banking accessible data. Note: Contact Support for fixes. 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:H/I:L/A:N).	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-FLEXC-011117/127

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2017-10363		
Glassfish Server					
NA	19-10-2017	5.8	Vulnerability in the Oracle GlassFish Server component of Oracle Fusion Middleware (subcomponent: Administration Graphical User Interface). The supported version that is affected is 3.1.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle GlassFish Server. 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 Oracle GlassFish Server accessible data as well as unauthorized read access to a subset of Oracle GlassFish Server accessible data. CVSS 3.0 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N). **CVE ID : CVE-2017-10400**	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-GLASS-011117/128
DoS	19-10-2017	6.8	Vulnerability in the Oracle GlassFish Server component of Oracle Fusion Middleware (subcomponent: Web Container). Supported versions that are affected are 3.0.1 and 3.1.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle GlassFish Server. 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 Oracle GlassFish Server accessible	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-GLASS-011117/129

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			data as well as unauthorized read access to a subset of Oracle GlassFish Server accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle GlassFish Server. CVSS 3.0 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L). **CVE ID : CVE-2017-10393**		
DoS	19-10-2017	6.8	Vulnerability in the Oracle GlassFish Server component of Oracle Fusion Middleware (subcomponent: Web Container). Supported versions that are affected are 3.0.1 and 3.1.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle GlassFish Server. 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 Oracle GlassFish Server accessible data as well as unauthorized read access to a subset of Oracle GlassFish Server accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle GlassFish Server. CVSS 3.0 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L). **CVE ID : CVE-2017-10385**	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-GLASS-011117/130
DoS	19-10-2017	7.5	Vulnerability in the Oracle GlassFish Server component of Oracle Fusion Middleware (subcomponent: Administration). Supported versions that are	http://www.oracle.com/technetwork/security-	A-ORA-GLASS-011117/131

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected are 3.0.1 and 3.1.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle GlassFish Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle GlassFish Server accessible data as well as unauthorized read access to a subset of Oracle GlassFish Server accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle GlassFish Server. CVSS 3.0 Base Score 7.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L). **CVE ID : CVE-2017-10391**	advisory/cpuoct2017-3236626.html	
Global Order Promising					
NA	19-10-2017	6.4	Vulnerability in the Oracle Global Order Promising component of Oracle E-Business Suite (subcomponent: Reschedule Sales Orders). 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 Global Order Promising. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Global Order Promising accessible data as well as unauthorized access to critical data or complete access to all Oracle Global Order Promising accessible data. CVSS 3.0 Base Score 9.1 (Confidentiality and	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-GLOBA-011117/132

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 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-2017-10329**		
Hospitality Cruise Affairwhere					
NA	19-10-2017	6.5	Vulnerability in the Oracle Hospitality Cruise AffairWhere component of Oracle Hospitality Applications (subcomponent: AffairWhere). Supported versions that are affected are 2.2.5.0, 2.2.6.0 and 2.2.7.0. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Hospitality Cruise AffairWhere Executeutes to compromise Oracle Hospitality Cruise AffairWhere. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Hospitality Cruise AffairWhere, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle Hospitality Cruise AffairWhere. 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-2017-10396**	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-HOSPI-011117/133
Hospitality Cruise Fleet Management					
NA	19-10-2017	3.2	Vulnerability in the Oracle Hospitality Cruise Fleet Management component of Oracle Hospitality Applications (subcomponent: BaseMasterPage). The supported version that is affected is 9.0.2.0. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Hospitality Cruise Fleet	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-HOSPI-011117/134

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Management Executeutes to compromise Oracle Hospitality Cruise Fleet Management. 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 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 8.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:N). **CVE ID : CVE-2017-10398**		
DoS	19-10-2017	3.5	Vulnerability in the Oracle Hospitality Cruise Fleet Management component of Oracle Hospitality Applications (subcomponent: GangwayActivityWebApp). The supported version that is affected is 9.0.2.0. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hospitality Cruise Fleet Management. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Hospitality Cruise Fleet Management. CVSS 3.0 Base Score 3.1 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2017-10399**	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-HOSPI-011117/135

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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	19-10-2017	5.5	Vulnerability in the Oracle Hospitality Cruise Fleet Management component of Oracle Hospitality Applications (subcomponent: GangwayActivityWebApp). The supported version that is affected is 9.0.2.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hospitality Cruise Fleet Management. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Hospitality Cruise Fleet Management accessible data as well as unauthorized read access to a subset of Oracle Hospitality Cruise Fleet 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-2017-10395**	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-HOSPI-011117/136
NA	19-10-2017	5.8	Vulnerability in the Oracle Hospitality Cruise Fleet Management component of Oracle Hospitality Applications (subcomponent: BaseMasterPage). The supported version that is affected is 9.0.2.0. Easily exploitable vulnerability allows unauthenticated 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	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-HOSPI-011117/137

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Hospitality Cruise Fleet Management accessible data as well as unauthorized read access to a subset of Oracle Hospitality Cruise Fleet 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-2017-10397**		
Hospitality Cruise Materials Management					
NA	19-10-2017	3.6	Vulnerability in the Oracle Hospitality Cruise Materials Management component of Oracle Hospitality Applications (subcomponent: MMS). The supported version that is affected is 7.30.564.0. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle Hospitality Cruise Materials Management Executeutes to compromise Oracle Hospitality Cruise Materials Management. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Hospitality Cruise Materials Management accessible data as well as unauthorized read access to a subset of Oracle Hospitality Cruise Materials Management accessible data. CVSS 3.0 Base Score 5.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N). **CVE ID : CVE-2017-10054**	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-HOSPI-011117/138
NA	19-10-2017	4.3	Vulnerability in the Oracle	http://w	A-ORA-

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Hospitality Cruise Materials Management component of Oracle Hospitality Applications (subcomponent: MMSUpdater). The supported version that is affected is 7.30.564.0. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Hospitality Cruise Materials Management Executeutes to compromise Oracle Hospitality Cruise Materials Management. While the vulnerability is in Oracle Hospitality Cruise Materials Management, 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 Hospitality Cruise Materials Management accessible data as well as unauthorized read access to a subset of Oracle Hospitality Cruise Materials Management accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Hospitality Cruise Materials Management. CVSS 3.0 Base Score 8.7 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:H/A:H). **CVE ID : CVE-2017-10401**	ww.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	HOSPI-011117/139
Hospitality Cruise Shipboard Property Management System					
DoS	19-10-2017	5.5	Vulnerability in the Oracle Hospitality Cruise Shipboard Property Management System component of Oracle Hospitality Applications (subcomponent: OHC DRS). The supported version that is affected is 8.0.2.0. Easily exploitable vulnerability allows	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-	A-ORA-HOSPI-011117/140

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			low privileged attacker with network access via HTTP to compromise Oracle Hospitality Cruise Shipboard Property Management System. While the vulnerability is in Oracle Hospitality Cruise Shipboard Property Management System, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Hospitality Cruise Shipboard Property Management System accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Hospitality Cruise Shipboard Property Management System. CVSS 3.0 Base Score 6.4 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:N/A:L). **CVE ID : CVE-2017-10361**	3236626.html	
Hospitality Guest Access					
NA	19-10-2017	4.9	Vulnerability in the Oracle Hospitality Guest Access component of Oracle Hospitality Applications (subcomponent: Base). Supported versions that are affected are 4.2.0 and 4.2.1. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hospitality Guest Access. 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 Oracle Hospitality Guest Access accessible data as well as unauthorized read access to a subset of Oracle	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-HOSPI-011117/141

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Hospitality Guest Access accessible data. CVSS 3.0 Base Score 4.6 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:L/A:N). **CVE ID : CVE-2017-10375**		
NA	19-10-2017	4.9	Vulnerability in the Oracle Hospitality Guest Access component of Oracle Hospitality Applications (subcomponent: Base). Supported versions that are affected are 4.2.0 and 4.2.1. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Hospitality Guest Access. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Hospitality Guest Access, 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 Guest Access accessible data as well as unauthorized update, insert or delete access to some of Oracle Hospitality Guest Access accessible data. CVSS 3.0 Base Score 6.9 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:C/C:H/I:L/A:N). **CVE ID : CVE-2017-10370**	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-HOSPI-011117/142
Gain Information	19-10-2017	5	Vulnerability in the Oracle Hospitality Guest Access component of Oracle Hospitality Applications (subcomponent: Interface). Supported versions that are affected are 4.2.0 and 4.2.1. Easily exploitable vulnerability allows unauthenticated attacker	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-	A-ORA-HOSPI-011117/143

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			with network access via HTTP to compromise Oracle Hospitality Guest Access. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Hospitality Guest Access 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-2017-10383**	3236626.html	
NA	19-10-2017	5.5	Vulnerability in the Oracle Hospitality Guest Access component of Oracle Hospitality Applications (subcomponent: Base). Supported versions that are affected are 4.2.0 and 4.2.1. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Hospitality Guest Access. While the vulnerability is in Oracle Hospitality Guest Access, 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 Hospitality Guest Access accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Hospitality Guest Access. CVSS 3.0 Base Score 8.7 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:C/C:N/I:H/A:H). **CVE ID : CVE-2017-10372**	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-HOSPI-011117/144
Hospitality Hotel Mobile					
NA	19-10-2017	3.5	Vulnerability in the Oracle Hospitality Hotel Mobile component of Oracle Hospitality	http://www.oracle.com/tec	A-ORA-HOSPI-011117/

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Applications (subcomponent: Suite8/RESTAPI). The supported version that is affected is 1.1. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hospitality Hotel Mobile. 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 Oracle Hospitality Hotel Mobile accessible data. CVSS 3.0 Base Score 3.5 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:L/A:N). **CVE ID : CVE-2017-10014**	hnetwork/security-advisory/cpuoct2017-3236626.html	145
DoS	19-10-2017	5.5	Vulnerability in the Oracle Hospitality Hotel Mobile component of Oracle Hospitality Applications (subcomponent: Suite8/RESTAPI). The supported version that is affected is 1.1. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hospitality Hotel Mobile. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hospitality Hotel Mobile accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Hospitality Hotel Mobile. CVSS 3.0 Base Score 7.1 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:L). **CVE ID : CVE-2017-10353**	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-HOSPI-011117/146
Hospitality Opera 5 Property Services					
Gain	19-10-2017	2.1	Vulnerability in the Oracle	http://w	A-ORA-

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information			Hospitality OPERA 5 Property Services component of Oracle Hospitality Applications (subcomponent: Folios). The supported version that is affected is 5.4.2.x through 5.5.1.x. Easily exploitable vulnerability allows physical access to compromise Oracle Hospitality OPERA 5 Property Services. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hospitality OPERA 5 Property Services accessible data. CVSS 3.0 Base Score 4.6 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2017-10197**	ww.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	HOSPI-011117/147
Hospitality Reporting And Analytics					
NA	19-10-2017	4.6	Vulnerability in the Oracle Hospitality Reporting and Analytics component of Oracle Hospitality Applications (subcomponent: iQuery). Supported versions that are affected are 8.5.1 and 9.0.0. Difficult to exploit vulnerability allows low privileged 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 of this vulnerability can result in takeover of Oracle Hospitality Reporting and Analytics. CVSS 3.0 Base Score 8.0 (Confidentiality,	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-HOSPI-011117/148

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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:H/PR:L/UI:R/S:C/C:H/I:H/A:H). **CVE ID : CVE-2017-10403**		
NA	19-10-2017	6.4	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. While the vulnerability is in Oracle Hospitality Reporting and Analytics, 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 Reporting and Analytics accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Hospitality Reporting and Analytics. CVSS 3.0 Base Score 10.0 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:H). **CVE ID : CVE-2017-10405**	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-HOSPI-011117/149
NA	19-10-2017	6.5	Vulnerability in the Oracle Hospitality Reporting and Analytics component of Oracle Hospitality Applications (subcomponent: iQuery). Supported versions that are affected are 8.5.1 and 9.0.0. Easily exploitable vulnerability allows low privileged attacker with	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.	A-ORA-HOSPI-011117/150

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 Hospitality Reporting and Analytics. While the vulnerability is in Oracle Hospitality Reporting and Analytics, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle Hospitality Reporting and Analytics. CVSS 3.0 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H). **CVE ID : CVE-2017-10404**	html	
NA	19-10-2017	7.5	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 unauthenticated attacker with network access via HTTP to compromise Oracle Hospitality Reporting and Analytics. While the vulnerability is in Oracle Hospitality Reporting and Analytics, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle Hospitality Reporting and Analytics. CVSS 3.0 Base Score 10.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H). **CVE ID : CVE-2017-10402**	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-HOSPI-011117/151
Hospitality Simphony					
Gain Information	19-10-2017	4.3	Vulnerability in the Oracle Hospitality Simphony component	http://www.oracl	A-ORA-HOSPI-

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of Oracle Hospitality Applications (subcomponent: Import/Export). Supported versions that are affected are 2.8 and 2.9. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hospitality Simphony. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hospitality Simphony accessible data. CVSS 3.0 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N). **CVE ID : CVE-2017-10343**	e.com/technetwork/security-advisory/cpuoct2017-3236626.html	011117/152
NA	19-10-2017	5.5	Vulnerability in the Oracle Hospitality Simphony component of Oracle Hospitality Applications (subcomponent: Service Host). Supported versions that are affected are 2.6, 2.7, 2.8 and 2.9. 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 update, insert or delete access to some of Oracle Hospitality Simphony accessible data as well as unauthorized read access to a subset of Oracle Hospitality Simphony 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-2017-10425**	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-HOSPI-011117/153

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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	19-10-2017	5.8	Vulnerability in the Oracle Hospitality Simphony component of Oracle Hospitality Applications (subcomponent: Engagement). Supported versions that are affected are 2.8 and 2.9. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hospitality Simphony. 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 Oracle Hospitality Simphony accessible data as well as unauthorized read access to a subset of Oracle Hospitality Simphony accessible data. CVSS 3.0 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N). **CVE ID : CVE-2017-10367**	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-HOSPI-011117/154
NA	19-10-2017	5.8	Vulnerability in the Oracle Hospitality Simphony component of Oracle Hospitality Applications (subcomponent: Import/Export). Supported versions that are affected are 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 access to all Oracle Hospitality Simphony accessible data as well as unauthorized update, insert or delete access to some of Oracle Hospitality Simphony accessible	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-HOSPI-011117/155

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			data. CVSS 3.0 Base Score 6.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N). **CVE ID : CVE-2017-10344**		
NA	19-10-2017	5.8	Vulnerability in the Oracle Hospitality Simphony component of Oracle Hospitality Applications (subcomponent: Import/Export). Supported versions that are affected are 2.8 and 2.9. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hospitality Simphony. 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 Oracle Hospitality Simphony accessible data as well as unauthorized read access to a subset of Oracle Hospitality Simphony accessible data. CVSS 3.0 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N). **CVE ID : CVE-2017-10340**	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-HOSPI-011117/156
Hospitality Suite8					
Gain Information	19-10-2017	2.1	Vulnerability in the Oracle Hospitality Suite8 component of Oracle Hospitality Applications (subcomponent: WebConnect). Supported versions that are affected are 8.10.1 and 8.10.2. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle Hospitality Suite8 Executeutes to compromise Oracle Hospitality Suite8. Successful	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-HOSPI-011117/157

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Hospitality Suite8 accessible data. CVSS 3.0 Base Score 4.0 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2017-10317**		
NA	19-10-2017	3.6	Vulnerability in the Oracle Hospitality Suite8 component of Oracle Hospitality Applications (subcomponent: PMS). Supported versions that are affected are 8.10.1 and 8.10.2. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle Hospitality Suite8 Executeutes to compromise Oracle Hospitality Suite8. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Hospitality Suite8 accessible data as well as unauthorized read access to a subset of Oracle Hospitality Suite8 accessible data. CVSS 3.0 Base Score 5.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N). **CVE ID : CVE-2017-10419**	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-HOSPI-011117/158
Gain Information	19-10-2017	4	Vulnerability in the Oracle Hospitality Suite8 component of Oracle Hospitality Applications (subcomponent: Leisure). Supported versions that are affected are 8.10.1 and 8.10.2. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hospitality Suite8. Successful attacks of this vulnerability can result in	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-HOSPI-011117/159

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthorized access to critical data or complete access to all Oracle Hospitality Suite8 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-2017-10421**		
Gain Information	19-10-2017	4	Vulnerability in the Oracle Hospitality Suite8 component of Oracle Hospitality Applications (subcomponent: WebConnect). Supported versions that are affected are 8.10.1 and 8.10.2. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hospitality Suite8. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hospitality Suite8 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-2017-10316**	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-HOSPI-011117/160
DoS	19-10-2017	4.1	Vulnerability in the Oracle Hospitality Suite8 component of Oracle Hospitality Applications (subcomponent: PMS). Supported versions that are affected are 8.10.1 and 8.10.2. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Hospitality Suite8 Executeutes to compromise Oracle Hospitality Suite8. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Hospitality Suite8, attacks may	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-HOSPI-011117/161

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Hospitality Suite8 accessible data as well as unauthorized read access to a subset of Oracle Hospitality Suite8 accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Hospitality Suite8. CVSS 3.0 Base Score 5.7 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:L). **CVE ID : CVE-2017-10389**		
Gain Information	19-10-2017	4.3	Vulnerability in the Oracle Hospitality Suite8 component of Oracle Hospitality Applications (subcomponent: WebConnect). Supported versions that are affected are 8.10.1 and 8.10.2. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hospitality Suite8. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hospitality Suite8 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-2017-10339**	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-HOSPI-011117/162
Gain Information	19-10-2017	4.3	Vulnerability in the Oracle Hospitality Suite8 component of Oracle Hospitality Applications (subcomponent: WebConnect). Supported versions that are affected are 8.10.1 and 8.10.2. Easily exploitable vulnerability	http://www.oracle.com/technetwork/security-advisory/cpuoct20	A-ORA-HOSPI-011117/163

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allows unauthenticated attacker with network access via HTTP to compromise Oracle Hospitality Suite8. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Hospitality Suite8, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Hospitality Suite8 accessible data. 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-2017-10318**	17-3236626.html	
Gain Information	19-10-2017	5	Vulnerability in the Oracle Hospitality Suite8 component of Oracle Hospitality Applications (subcomponent: Leisure). Supported versions that are affected are 8.10.1 and 8.10.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hospitality Suite8. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Hospitality Suite8 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-2017-10319**	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-HOSPI-011117/164
DoS	19-10-2017	5.5	Vulnerability in the Oracle Hospitality Suite8 component of Oracle Hospitality Applications (subcomponent: Leisure). Supported versions that are affected are 8.10.1 and 8.10.2. Easily exploitable vulnerability	http://www.oracle.com/technetwork/security-advisory/cpuoct20	A-ORA-HOSPI-011117/165

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 low privileged attacker with network access via HTTP to compromise Oracle Hospitality Suite8. While the vulnerability is in Oracle Hospitality Suite8, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Hospitality Suite8 accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Hospitality Suite8. CVSS 3.0 Base Score 6.4 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:N/I:L/A:L). **CVE ID : CVE-2017-10420**	17-3236626.html	
DoS Gain Information	19-10-2017	5.5	Vulnerability in the Oracle Hospitality Suite8 component of Oracle Hospitality Applications (subcomponent: Leisure). Supported versions that are affected are 8.10.1 and 8.10.2. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hospitality Suite8. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Hospitality Suite8 accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Hospitality Suite8. CVSS 3.0 Base Score 5.4 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:L). **CVE ID : CVE-2017-10337**	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-HOSPI-011117/166
NA	19-10-2017	5.8	Vulnerability in the Oracle Hospitality Suite8 component of Oracle Hospitality Applications	http://www.oracle.com/tec	A-ORA-HOSPI-011117/

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(subcomponent: WebConnect). Supported versions that are affected are 8.10.1 and 8.10.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hospitality Suite8. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Hospitality Suite8, 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 Suite8 accessible data as well as unauthorized update, insert or delete access to some of Oracle Hospitality Suite8 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-2017-10050**	hnetwork/security-advisory/cpuoct2017-3236626.html	167
Hyperion Bi+					
NA	19-10-2017	5.8	Vulnerability in the Oracle Hyperion BI+ component of Oracle Hyperion (subcomponent: UI and Visualization). The supported version that is affected is 11.1.2.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle 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 Oracle Hyperion BI+ accessible data as well as unauthorized read	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-HYPER-011117/168

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 a subset of Oracle Hyperion BI+ accessible data. CVSS 3.0 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N). **CVE ID : CVE-2017-10359**		
NA	19-10-2017	5.8	Vulnerability in the Oracle Hyperion BI+ component of Oracle Hyperion (subcomponent: UI and Visualization). The supported version that is affected is 11.1.2.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hyperion BI+. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hyperion BI+ accessible data as well as unauthorized update, insert or delete access to some of Oracle Hyperion BI+ accessible data. CVSS 3.0 Base Score 7.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:L/A:N). **CVE ID : CVE-2017-10312**	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-HYPER-011117/169
Hyperion Financial Reporting					
Gain Information	19-10-2017	5	Vulnerability in the Oracle Hyperion Financial Reporting component of Oracle Hyperion (subcomponent: Security Models). The supported version that is affected is 11.1.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hyperion Financial Reporting. Successful attacks of this vulnerability can	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-HYPER-011117/170

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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
			result in unauthorized access to critical data or complete access to all Oracle Hyperion Financial Reporting 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-2017-10310**		
NA	19-10-2017	5.5	Vulnerability in the Oracle Hyperion Financial Reporting component of Oracle Hyperion (subcomponent: Workspace). The supported version that is affected is 11.1.2. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hyperion Financial Reporting. While the vulnerability is in Oracle Hyperion Financial Reporting, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Hyperion Financial Reporting accessible data as well as unauthorized read access to a subset of Oracle Hyperion Financial Reporting 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-2017-10358**	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-HYPER-011117/171
Identity Manager Connector					
NA	19-10-2017	3.3	Vulnerability in the Oracle Identity Manager Connector component of Oracle Fusion Middleware (subcomponent: Microsoft Active Directory). The supported version that is affected is 9.1.1.5.0. Easily exploitable vulnerability allows unauthenticated attacker with	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-	A-ORA-IDENT-011117/172

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			logon to the infrastructure where Oracle Identity Manager Connector Execute to compromise Oracle Identity Manager Connector. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Identity Manager Connector, 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 Identity Manager Connector accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Identity Manager Connector. CVSS 3.0 Base Score 8.2 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:C/C:N/I:H/A:H). **CVE ID : CVE-2017-10270**	3236626.html	
Interaction Center Intelligence					
NA	19-10-2017	5.8	Vulnerability in the Oracle Interaction Center Intelligence component of Oracle E-Business Suite (subcomponent: Setup). Supported versions that are affected are 12.1.1, 12.1.2 and 12.1.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Interaction Center Intelligence. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Interaction Center Intelligence, attacks may significantly impact additional products. Successful	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-INTER-011117/173

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Interaction Center Intelligence accessible data as well as unauthorized update, insert or delete access to some of Oracle Interaction Center Intelligence 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-2017-10303**		
Iplanet Web Server					
NA	19-10-2017	5.8	Vulnerability in the Oracle iPlanet Web Server component of Oracle Fusion Middleware (subcomponent: Admin Graphical User Interface). The supported version that is affected is 7.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle iPlanet Web Server. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle iPlanet Web Server, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle iPlanet Web Server accessible data as well as unauthorized read access to a subset of Oracle iPlanet Web Server accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2017-10055**	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-IPLAN-011117/174
Istore					

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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	19-10-2017	5.8	Vulnerability in the Oracle iStore component of Oracle E-Business Suite (subcomponent: Checkout and Order Placement). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6 and 12.2.7. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle iStore. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle iStore, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle iStore accessible data as well as unauthorized update, insert or delete access to some of Oracle iStore accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N). **CVE ID : CVE-2017-10414**	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-ISTOR-011117/175
NA	19-10-2017	5.8	Vulnerability in the Oracle iStore component of Oracle E-Business Suite (subcomponent: Merchant UI). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6 and 12.2.7. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle iStore. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle iStore, attacks may significantly impact	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-ISTOR-011117/176

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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
			additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle iStore accessible data as well as unauthorized update, insert or delete access to some of Oracle iStore accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N). **CVE ID : CVE-2017-10409**		
Isupport					
NA	19-10-2017	5.8	Vulnerability in the Oracle iSupport component of Oracle E-Business Suite (subcomponent: Others). 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 iSupport. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle iSupport, 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 iSupport accessible data as well as unauthorized update, insert or delete access to some of Oracle iSupport 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-2017-10415**	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-ISUPP-011117/177
Java Advanced Management Console					

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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	19-10-2017	4	Vulnerability in the Java Advanced Management Console component of Oracle Java SE (subcomponent: Server). The supported version that is affected is Java Advanced Management Console: 2.7. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Java Advanced Management Console. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java Advanced Management Console, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java Advanced Management Console accessible data as well as unauthorized read access to a subset of Java Advanced Management Console accessible data. CVSS 3.0 Base Score 4.7 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2017-10380**	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-JAVA - 011117/178
NA	19-10-2017	4.3	Vulnerability in the Java Advanced Management Console component of Oracle Java SE (subcomponent: Server). The supported version that is affected is Java Advanced Management Console: 2.7. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java Advanced Management Console. Successful attacks of this vulnerability can result in unauthorized update, insert or	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-JAVA - 011117/179

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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
			delete access to some of Java Advanced Management Console 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 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2017-10341**		
NA	19-10-2017	4.9	Vulnerability in the Java Advanced Management Console component of Oracle Java SE (subcomponent: Sever). The supported version that is affected is Java Advanced Management Console: 2.7. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Java Advanced Management Console. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java Advanced Management Console, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java Advanced Management Console accessible data as well as unauthorized read access to a subset of Java Advanced	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-JAVA - 011117/180

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Management Console accessible data. CVSS 3.0 Base Score 4.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2017-10386**		
DoS	19-10-2017	5	Vulnerability in the Java Advanced Management Console component of Oracle Java SE (subcomponent: Server). The supported version that is affected is Java Advanced Management Console: 2.7. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java Advanced Management Console. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java Advanced Management Console. 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-2017-10342**	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-JAVA - 011117/181
JDK;JRE					
Gain Information	19-10-2017	2.1	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: Security). Supported versions that are affected are Java SE: 6u161, 7u151, 8u144 and 9; Java SE Embedded: 8u144; JRockit: R28.3.15. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where Java SE, Java SE Embedded, JRockit Executeutes to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-JDK;J-011117/182

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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
			unauthorized access to critical data or complete access to all Java SE, Java SE Embedded, JRockit accessible data. Note: 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 6.2 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2017-10356**		
NA	19-10-2017	4	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: Smart Card IO). Supported versions that are affected are Java SE: 6u161, 7u151, 8u144 and 9. 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. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Java SE accessible data as well as unauthorized access to critical data or complete access to all 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	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-JDK;J-011117/183

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:N). **CVE ID : CVE-2017-10274**		
DoS	19-10-2017	5	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Serialization). Supported versions that are affected are Java SE: 6u161, 7u151, 8u144 and 9; Java SE Embedded: 8u144. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. 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 applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-JDK;J-011117/184

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2017-10357		
DoS	19-10-2017	5	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: JAX-WS). Supported versions that are affected are Java SE: 7u151, 8u144 and 9; Java SE Embedded: 8u144. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. 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 applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 5.3 (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-2017-10350**	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-JDK;J-011117/185
DoS	19-10-2017	5	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: JAXP). Supported versions that are affected are Java SE: 6u161, 7u151, 8u144 and 9; Java SE Embedded: 8u144. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-JDK;J-011117/186

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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
			protocols to compromise Java SE, Java SE Embedded. 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 applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 5.3 (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-2017-10349**		
DoS	19-10-2017	5	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Libraries). Supported versions that are affected are Java SE: 6u161, 7u151, 8u144 and 9; Java SE Embedded: 8u144. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. 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 applications or sandboxed Java	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-JDK;J-011117/187

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 5.3 (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-2017-10348**		
DoS	19-10-2017	5	Vulnerability in the Java SE, JRockit component of Oracle Java SE (subcomponent: Serialization). Supported versions that are affected are Java SE: 6u161, 7u151, 8u144 and 9; Java SE Embedded: 8u144. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, JRockit. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, JRockit. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-JDK;J-011117/188

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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
			S:U/C:N/I:N/A:L). **CVE ID : CVE-2017-10347**		
NA	19-10-2017	5.1	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Libraries). Supported versions that are affected are Java SE: 6u161, 7u151, 8u144 and 9; Java SE Embedded: 8u144. Difficult to exploit vulnerability allows unauthenticated attacker with network access via Kerberos 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 takeover of Java SE, Java SE Embedded. Note: Applies to the Java SE Kerberos client. CVSS 3.0 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2017-10388**	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-JDK;J-011117/189
NA	19-10-2017	5.8	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: Javadoc). Supported versions that are affected are Java SE: 6u161, 7u151, 8u144 and 9. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP 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 unauthorized update, insert or delete access to some of	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-JDK;J-011117/190

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Java SE accessible data as well as 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 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-2017-10293**		
NA	19-10-2017	6.8	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Hotspot). Supported versions that are affected are Java SE: 6u161, 7u151, 8u144 and 9; Java SE Embedded: 8u144. 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 and while the vulnerability is in Java SE, Java SE Embedded, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-JDK;J-011117/191

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 9.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H). **CVE ID : CVE-2017-10346**		
DoS	19-10-2017	6.8	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: Deployment). Supported versions that are affected are Java SE: 8u144 and 9. Easily exploitable 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 unauthorized update, insert or delete access to some of Java SE accessible data as well as unauthorized read access to a subset of Java SE accessible data and unauthorized ability to cause a partial denial of service (partial DOS) 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	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-JDK;J-011117/192

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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
			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 7.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:L). **CVE ID : CVE-2017-10309**		
NA	19-10-2017	6.8	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: RMI). Supported versions that are affected are Java SE: 6u161, 7u151, 8u144 and 9; Java SE Embedded: 8u144. 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 and while the vulnerability is in Java SE, Java SE Embedded, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE, Java SE Embedded. Note: This 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	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-JDK;J-011117/193

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 9.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H). **CVE ID : CVE-2017-10285**		
JDK;JRE;Jrockit					
DoS	19-10-2017	2.6	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: Serialization). Supported versions that are affected are Java SE: 6u161, 7u151, 8u144 and 9; Java SE Embedded: 8u144; JRockit: R28.3.15. 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. 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 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 3.1 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:N/A:L). **CVE ID : CVE-2017-10345**	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-JDK;J-011117/194

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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	19-10-2017	4.3	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: Networking). Supported versions that are affected are Java SE: 6u161, 7u151, 8u144 and 9; Java SE Embedded: 8u144; JRockit: R28.3.15. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Java SE, Java SE Embedded, JRockit. While the vulnerability is in Java SE, Java SE Embedded, JRockit, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Java SE Embedded, JRockit accessible data. Note: 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 4.0 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:N/I:L/A:N). **CVE ID : CVE-2017-10295**	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-JDK;J-011117/195
DoS	19-10-2017	5	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: Networking). Supported versions that are affected are Java SE: 6u161, 7u151, 8u144 and 9; Java SE Embedded: 8u144; JRockit: R28.3.15. Easily exploitable vulnerability allows unauthenticated attacker with	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-JDK;J-011117/196

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 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/C:N/I:N/A:L). **CVE ID : CVE-2017-10355**		
DoS	19-10-2017	5	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: Serialization). Supported versions that are affected are Java SE: 6u161, 7u151, 8u144 and 9; Java SE Embedded: 8u144; JRockit: R28.3.15. 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 can be exploited through sandboxed Java Web Start applications and sandboxed Java	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-JDK;J-011117/197

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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/C:N/I:N/A:L). **CVE ID : CVE-2017-10281**		
Knowledge Management					
NA	19-10-2017	5.8	Vulnerability in the Oracle Knowledge Management component of Oracle E-Business Suite (subcomponent: User Interface). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6 and 12.2.7. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Knowledge Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Knowledge 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 Knowledge Management accessible data as well as unauthorized update, insert or delete access to some of Oracle Knowledge 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-2017-10412**	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-KNOWL-011117/198

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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	19-10-2017	5.8	Vulnerability in the Oracle Knowledge Management component of Oracle E-Business Suite (subcomponent: User Interface). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6 and 12.2.7. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Knowledge Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Knowledge 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 Knowledge Management accessible data as well as unauthorized update, insert or delete access to some of Oracle Knowledge 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-2017-10411**	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-KNOWL-011117/199
NA	19-10-2017	5.8	Vulnerability in the Oracle Knowledge Management component of Oracle E-Business Suite (subcomponent: Search). 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 Knowledge Management. Successful attacks	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-KNOWL-011117/200

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			require human interaction from a person other than the attacker and while the vulnerability is in Oracle Knowledge 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 Knowledge Management accessible data as well as unauthorized update, insert or delete access to some of Oracle Knowledge 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-2017-10410**		
Mobile Field Service					
NA	19-10-2017	5.8	Vulnerability in the Oracle Mobile Field Service component of Oracle E-Business Suite (subcomponent: Multiplatform Based on HTML5). 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 Mobile Field Service. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Mobile Field Service, 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 Mobile Field Service accessible data as well as unauthorized update, insert or	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-MOBIL-011117/201

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			delete access to some of Oracle Mobile Field Service 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-2017-10413**		
Mysql					
Gain Information	19-10-2017	1.5	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 5.5.57 and earlier, 5.6.37 and earlier and 5.7.19 and earlier. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Server Executeutes 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 4.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2017-10268**	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-MYSQL-011117/202
NA	19-10-2017	1.7	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.6.37 and earlier and 5.7.19 and earlier. 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	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-MYSQL-011117/203

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2017-10294**		
NA	19-10-2017	3.5	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: InnoDB). Supported versions that are affected are 5.6.37 and earlier and 5.7.19 and earlier. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2017-10286**	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-MYSQL-011117/204
NA	19-10-2017	3.5	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Performance Schema). Supported versions that are affected are 5.6.37 and earlier and 5.7.19 and earlier. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-MYSQL-011117/205

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			S:U/C:N/I:N/A:H). **CVE ID : CVE-2017-10283**		
NA	19-10-2017	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 5.5.57 and earlier 5.6.37 and earlier 5.7.19 and earlier. 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-2017-10384**	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-MYSQL-011117/206
Gain Information	19-10-2017	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Client programs). Supported versions that are affected are 5.5.57 and earlier, 5.6.37 and earlier and 5.7.19 and earlier. 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 access to critical data or complete access to all MySQL Server 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-2017-10379**	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-MYSQL-011117/207
NA	19-10-2017	4	Vulnerability in the MySQL Server component of Oracle MySQL	http://www.oracl	A-ORA-MYSQL-

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(subcomponent: Server: Optimizer). Supported versions that are affected are 5.5.57 and earlier, 5.6.37 and earlier and 5.7.11 and earlier. 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-2017-10378**	e.com/technetwork/security-advisory/cpuoct2017-3236626.html	011117/208
NA	19-10-2017	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: InnoDB). Supported versions that are affected are 5.7.19 and earlier. 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-2017-10320**	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-MYSQL-011117/209
NA	19-10-2017	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Memcached). Supported versions that are affected are 5.6.37 and earlier and 5.7.19 and earlier.	http://www.oracle.com/technetwork/security-advisory/	A-ORA-MYSQL-011117/210

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2017-10314**	cpuoct2017-3236626.html	
NA	19-10-2017	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Group Replication GCS). Supported versions that are affected are 5.7.19 and earlier. 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-2017-10313**	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-MYSQL-011117/211
NA	19-10-2017	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: FTS). Supported versions that are affected are 5.7.19 and earlier. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-MYSQL-011117/212

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 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-2017-10311**		
NA	19-10-2017	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DML). Supported versions that are affected are 5.7.18 and earlier. 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-2017-10296**	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-MYSQL-011117/213
NA	19-10-2017	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Stored Procedure). Supported versions that are affected are 5.7.18 and earlier. 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	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-MYSQL-011117/214

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2017-10284**		
NA	19-10-2017	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.6.36 and earlier and 5.7.18 and earlier. 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-2017-10279**	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-MYSQL-011117/215
NA	19-10-2017	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.6.37 and earlier and 5.7.19 and earlier. 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).	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-MYSQL-011117/216

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2017-10227		
NA	19-10-2017	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.7.19 and earlier. 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-2017-10167**	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-MYSQL-011117/217
NA	19-10-2017	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 5.7.19 and earlier. 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-2017-10165**	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-MYSQL-011117/218
NA	19-10-2017	5	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: FTS). Supported versions that are	http://www.oracle.com/technetwork	A-ORA-MYSQL-011117/219

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected are 5.6.37 and earlier and 5.7.19 and earlier. 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-2017-10276**	/security-advisory/cpuoct2017-3236626.html	
NA	19-10-2017	5	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Pluggable Auth). Supported versions that are affected are 5.6.37 and earlier and 5.7.19 and earlier. 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-2017-10155**	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-MYSQL-011117/220
DoS	19-10-2017	5.5	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: InnoDB). Supported versions that are affected are 5.7.18 and earlier. Easily exploitable vulnerability allows high privileged attacker with network access via multiple	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-	A-ORA-MYSQL-011117/221

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Server. CVSS 3.0 Base Score 3.8 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:L). **CVE ID : CVE-2017-10365**	3236626.html	
Mysql Connector/net					
DoS	19-10-2017	5	Vulnerability in the MySQL Connectors component of Oracle MySQL (subcomponent: Connector/Net). Supported versions that are affected are 6.9.9 and earlier. Easily exploitable vulnerability allows 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 partial denial of service (partial DOS) of MySQL Connectors. 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-2017-10203**	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-MYSQL-011117/222
NA	19-10-2017	5.8	Vulnerability in the MySQL Connectors component of Oracle MySQL (subcomponent: Connector/Net). Supported versions that are affected are 6.9.9 and earlier. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Connectors. Successful attacks	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-MYSQL-011117/223

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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
			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 MySQL Connectors accessible data as well as unauthorized read access to a subset of MySQL Connectors accessible data. CVSS 3.0 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N). **CVE ID : CVE-2017-10277**		
Mysql Enterprise Monitor					
NA	19-10-2017	6.8	Vulnerability in the MySQL Enterprise Monitor component of Oracle MySQL (subcomponent: Monitoring: Web). Supported versions that are affected are 3.2.8.2223 and earlier, 3.3.4.3247 and earlier and 3.4.2.4181 and earlier. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Enterprise Monitor. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Enterprise Monitor. 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-2017-10424**	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-MYSQL-011117/224
Outside In Technology					
Execute Code	19-10-2017	2.7	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). The supported version	http://www.oracle.com/technetwork/security-	A-ORA-OUTSI-011117/225

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			that is affected is 8.5.3.0. Easily exploitable vulnerability allows low privileged attacker with access to the physical communication segment attached to the hardware where the Oracle Outside In Technology Execute utes to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 5.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2017-10051**	advisory/cpuoct2017-3236626.html	
Peoplesoft Enterprise Fin Staffing Front Office					
Gain Information	19-10-2017	4	Vulnerability in the PeopleSoft Enterprise FSCM component of Oracle PeopleSoft Products (subcomponent: Staffing Front Office). 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 FSCM. Successful attacks of this vulnerability can result in unauthorized read access to a subset of PeopleSoft Enterprise FSCM accessible data. CVSS 3.0 Base Score 4.3	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-PEOPL-011117/226

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 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-2017-10164**		
Peoplesoft Enterprise Human Capital Management Human Resources					
NA	19-10-2017	4.9	Vulnerability in the PeopleSoft Enterprise HCM 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. 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 PeopleSoft Enterprise HCM accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise HCM accessible data. CVSS 3.0 Base Score 4.6 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:L/A:N). **CVE ID : CVE-2017-10306**	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-PEOPL-011117/227
NA	19-10-2017	4.9	Vulnerability in the PeopleSoft Enterprise HCM 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. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise HCM,	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-PEOPL-011117/228

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise HCM accessible data. CVSS 3.0 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2017-10304**		
Peoplesoft Enterprise Peopletools					
Gain Information	19-10-2017	2.1	Vulnerability in the PeopleSoft Enterprise PT PeopleTools component of Oracle PeopleSoft Products (subcomponent: Application Server). Supported versions that are affected are 8.54, 8.55 and 8.56. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where PeopleSoft Enterprise PT PeopleTools Executeutes to compromise PeopleSoft Enterprise PT PeopleTools. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all PeopleSoft Enterprise PT PeopleTools accessible data. CVSS 3.0 Base Score 6.2 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2017-10351**	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-PEOPL-011117/229
Gain Information	19-10-2017	4.3	Vulnerability in the PeopleSoft Enterprise PeopleTools component of Oracle PeopleSoft Products (subcomponent: Updates Change Assistant). The supported version that is affected is 8.54.	http://www.oracle.com/technetwork/security-advisory/	A-ORA-PEOPL-011117/230

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Difficult to exploit 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 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-2017-10422**	cpuoct2017-3236626.html	
NA	19-10-2017	4.3	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 and while the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.0 Base Score 4.7 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:L/A:N). **CVE ID : CVE-2017-10382**	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-PEOPL-011117/231
Gain Information	19-10-2017	5	Vulnerability in the PeopleSoft Enterprise PT PeopleTools	http://www.oracl	A-ORA-PEOPL-

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			component of Oracle PeopleSoft Products (subcomponent: Health Center). Supported versions that are affected are 8.55 and 8.56. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PT PeopleTools. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all PeopleSoft Enterprise PT 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-2017-10373**	e.com/technetwork/security-advisory/cpuoct2017-3236626.html	011117/232
Gain Information	19-10-2017	5	Vulnerability in the PeopleSoft Enterprise PT PeopleTools component of Oracle PeopleSoft Products (subcomponent: Elastic Search). Supported versions that are affected are 8.55 and 8.56. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PT PeopleTools. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all PeopleSoft Enterprise PT 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-2017-10335**	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-PEOPL-011117/233
Gain Information	19-10-2017	5	Vulnerability in the PeopleSoft Enterprise PeopleTools component of Oracle PeopleSoft Products (subcomponent: Test Framework). Supported versions that are affected are 8.54, 8.55 and	http://www.oracle.com/technetwork/security-advisory/	A-ORA-PEOPL-011117/234

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2017-10280**	cpuoct2017-3236626.html	
NA	19-10-2017	5.5	Vulnerability in the PeopleSoft Enterprise PT PeopleTools component of Oracle PeopleSoft Products (subcomponent: PeopleSoft CDA). The supported version that is affected is 8.56. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise PT PeopleTools. While the vulnerability is in PeopleSoft Enterprise PT PeopleTools, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PT PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PT PeopleTools 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-2017-10418**	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-PEOPL-011117/235
DoS	19-10-2017	5.5	Vulnerability in the PeopleSoft Enterprise PeopleTools	http://www.oracl	A-ORA-PEOPL-

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			component of Oracle PeopleSoft Products (subcomponent: Security). 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 update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of PeopleSoft Enterprise PeopleTools. CVSS 3.0 Base Score 5.4 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:L). **CVE ID : CVE-2017-10394**	e.com/technetwork/security-advisory/cpuoct2017-3236626.html	011117/236
NA	19-10-2017	5.5	Vulnerability in the PeopleSoft Enterprise PeopleTools component of Oracle PeopleSoft Products (subcomponent: Updates Environment Mgmt). 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 creation, deletion or modification access to critical data or all PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized access to critical data or complete access to all PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.0 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-PEOPL-011117/237

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			S:U/C:H/I:H/A:N). **CVE ID : CVE-2017-10364**		
NA	19-10-2017	5.8	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 and while the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2017-10406**	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-PEOPL-011117/238
NA	19-10-2017	5.8	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	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-PEOPL-011117/239

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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
			PeopleTools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2017-10381**		
NA	19-10-2017	5.8	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 unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-PEOPL-011117/240

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2017-10327**		
NA	19-10-2017	5.8	Vulnerability in the PeopleSoft Enterprise PeopleTools component of Oracle PeopleSoft Products (subcomponent: Core). 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 and while the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2017-10158**	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-PEOPL-011117/241
DoS	19-10-2017	6.4	Vulnerability in the PeopleSoft Enterprise PeopleTools component of Oracle PeopleSoft Products (subcomponent: Sawbridge). Supported versions that are affected are 8.54, 8.55 and	http://www.oracle.com/technetwork/security-advisory/	A-ORA-PEOPL-011117/242

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			8.56. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. While the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of PeopleSoft Enterprise PeopleTools. CVSS 3.0 Base Score 7.2 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:N/A:L). **CVE ID : CVE-2017-10362**	cpuoct2017-3236626.html	
NA	19-10-2017	7.5	Vulnerability in the PeopleSoft Enterprise PT PeopleTools component of Oracle PeopleSoft Products (subcomponent: Performance Monitor). 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 PT PeopleTools. Successful attacks of this vulnerability can result in takeover of PeopleSoft Enterprise PT PeopleTools. CVSS 3.0 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H). **CVE ID : CVE-2017-10366**	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-PEOPL-011117/243
Peoplesoft Enterprise Prtl Interaction Hub					
NA	19-10-2017	5.8	Vulnerability in the PeopleSoft	http://w	A-ORA-

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PRTL Interaction Hub. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise PRTL Interaction Hub, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all PeopleSoft Enterprise PRTL Interaction Hub accessible data as well as unauthorized update, insert or delete access to some of PeopleSoft Enterprise PRTL Interaction Hub 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-2017-10354**	ww.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	PEOPL-011117/244
NA	19-10-2017	5.8	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 unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PRTL Interaction Hub. Successful attacks require human interaction from a person other than the attacker and while the	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-PEOPL-011117/245

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is in PeopleSoft Enterprise PRTL Interaction Hub, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all PeopleSoft Enterprise PRTL Interaction Hub accessible data as well as unauthorized update, insert or delete access to some of PeopleSoft Enterprise PRTL Interaction Hub 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-2017-10338**		
Peoplesoft Enterprise Scm Eprocurement					
NA	19-10-2017	5.8	Vulnerability in the PeopleSoft Enterprise SCM eProcurement component of Oracle PeopleSoft Products (subcomponent: Manage Requisition Status). Supported versions that are affected are 9.1.00 and 9.2.00. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise SCM eProcurement. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise SCM eProcurement, 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 SCM eProcurement accessible data as well as unauthorized read access to a subset of PeopleSoft	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-PEOPL-011117/246

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Enterprise SCM eProcurement 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-2017-10368**		
Peoplesoft Enterprise Scm Strategic Sourcing					
Gain Information	19-10-2017	5	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 Enterprise FSCM. Successful attacks of this vulnerability can result in unauthorized read access to a subset of PeopleSoft Enterprise FSCM 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-2017-10287**	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-PEOPL-011117/247
Peoplesoft Enterprise Staffing Front Office					
NA	19-10-2017	4	Vulnerability in the PeopleSoft Enterprise FSCM component of Oracle PeopleSoft Products (subcomponent: Staffing Front Office). The supported version that is affected is 9.2. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise FSCM. Successful attacks of this vulnerability can result in unauthorized read access to a subset of PeopleSoft Enterprise FSCM accessible data. CVSS 3.0 Base Score 2.7 (Confidentiality impacts). CVSS Vector:	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-PEOPL-011117/248

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2017-10426**		
Retail Back Office					
NA	19-10-2017	4.9	Vulnerability in the Oracle Retail Back Office component of Oracle Retail Applications (subcomponent: Security). Supported versions that are affected are 13.2, 13.3, 13.4, 14.0 and 14.1. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Retail Back Office. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Retail Back Office, 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 Back Office accessible data as well as unauthorized read access to a subset of Oracle Retail Back Office accessible data. CVSS 3.0 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2017-10423**	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-RETAI-011117/249
Retail Point-of-service					
NA	19-10-2017	5.5	Vulnerability in the Oracle Retail Point-of-Service component of Oracle Retail Applications (subcomponent: Security). Supported versions that are affected are 13.2, 13.3, 13.4, 14.0 and 14.1. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Retail Point-of-Service. While the	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-RETAI-011117/250

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is in Oracle Retail Point-of-Service, 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 Retail Point-of-Service accessible data as well as unauthorized read access to a subset of Oracle Retail Point-of-Service accessible data. CVSS 3.0 Base Score 8.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:H/A:N). **CVE ID : CVE-2017-10065**		
Retail Xstore Point Of Service					
DoS	19-10-2017	6.8	Vulnerability in the Oracle Retail Xstore Point of Service component of Oracle Retail Applications (subcomponent: Point of Sale). Supported versions that are affected are 6.0.11, 6.5.11, 7.0.6, 7.1.6 and 15.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Retail Xstore Point of Service. While the vulnerability is in Oracle Retail Xstore Point of Service, 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 Xstore Point of Service accessible data as well as unauthorized read access to a subset of Oracle Retail Xstore Point of Service accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Retail Xstore Point of Service. CVSS 3.0 Base Score 6.5	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-RETAI-011117/251

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:L/I:L/A:L). **CVE ID : CVE-2017-10427**		
Security Service;Security Service Fmw					
NA	19-10-2017	4.3	Vulnerability in the Oracle Security Service component of Oracle Fusion Middleware (subcomponent: C Oracle SSL API). Supported versions that are affected are FMW: 11.1.1.9.0 and 12.1.3.0.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Oracle Security Service. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Security Service accessible data. CVSS 3.0 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2017-10166**	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-SECUR-011117/252
Siebel Core-server Framework					
NA	19-10-2017	5.5	Vulnerability in the Siebel Core - Server Framework component of Oracle Siebel CRM (subcomponent: Services). 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 Core - Server Framework. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Siebel Core - Server Framework accessible data as well as unauthorized read access to a subset of Siebel Core - Server	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-SIEBE-011117/253

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Framework 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-2017-10162**		
Siebel Customer Relationship Management Desktop					
Gain Information	19-10-2017	5	Vulnerability in the Siebel CRM Desktop component of Oracle Siebel CRM (subcomponent: Siebel Business Service Issues). Supported versions that are affected are 16.0 and 17.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Siebel CRM Desktop. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Siebel CRM Desktop 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-2017-10300**	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-SIEBE-011117/254
Siebel Ui Framework					
DoS	19-10-2017	5	Vulnerability in the Siebel UI Framework component of Oracle Siebel CRM (subcomponent: UIF Open UI). Supported versions that are affected are 16.0 and 17.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Siebel UI Framework. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Siebel UI Framework. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector:	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-SIEBE-011117/255

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2017-10264**		
NA	19-10-2017	5.8	Vulnerability in the Siebel UI Framework component of Oracle Siebel CRM (subcomponent: UIF Open UI). Supported versions that are affected are 16.0 and 17.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Siebel UI Framework. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Siebel UI Framework, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Siebel UI Framework accessible data as well as unauthorized read access to a subset of Siebel UI 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-2017-10315**	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-SIEBE-011117/256
NA	19-10-2017	5.8	Vulnerability in the Siebel UI Framework component of Oracle Siebel CRM (subcomponent: UIF Open UI). Supported versions that are affected are 16.0 and 17.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Siebel UI Framework. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Siebel UI Framework, attacks may significantly impact additional	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-SIEBE-011117/257

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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
			products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Siebel UI Framework accessible data as well as unauthorized read access to a subset of Siebel UI 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-2017-10302**		
NA	19-10-2017	5.8	Vulnerability in the Siebel UI Framework component of Oracle Siebel CRM (subcomponent: UIF Open UI). Supported versions that are affected are 16.0 and 17.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Siebel UI Framework. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Siebel UI Framework, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Siebel UI Framework accessible data as well as unauthorized update, insert or delete access to some of Siebel UI Framework 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-2017-10263**	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-SIEBE-011117/258
DoS	19-10-2017	6.5	Vulnerability in the Siebel UI Framework component of Oracle Siebel CRM (subcomponent: EAI). Supported versions that are	http://www.oracle.com/technetwork	A-ORA-SIEBE-011117/259

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected are 16.0 and 17.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Siebel UI Framework. While the vulnerability is in Siebel UI Framework, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Siebel UI Framework accessible data as well as unauthorized read access to a subset of Siebel UI Framework accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Siebel UI Framework. 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-2017-10333**	/security-advisory/cpuoct2017-3236626.html	
Soa Suite					
NA	19-10-2017	5.8	Vulnerability in the Oracle SOA Suite component of Oracle Fusion Middleware (subcomponent: Fabric Layer). The supported version that is affected is 11.1.1.7.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle SOA Suite. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle SOA Suite, 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 SOA Suite accessible data as	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-SOA S-011117/260

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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
			well as unauthorized update, insert or delete access to some of Oracle SOA Suite 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-2017-10026**		
Solaris Cluster					
DoS	19-10-2017	4.4	Vulnerability in the Solaris Cluster component of Oracle Sun Systems Products Suite (subcomponent: HA for MySQL). Supported versions that are affected are 3.3 and 4.3. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where Solaris Cluster Executeutes to compromise Solaris Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Solaris Cluster accessible data as well as unauthorized access to critical data or complete access to all Solaris Cluster accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Solaris Cluster. CVSS 3.0 Base Score 7.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:L). **CVE ID : CVE-2017-3588**	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-SOLAR-011117/261
Sparc-sun System Firmware					
NA	19-10-2017	4.9	Vulnerability in the SPARC M7, T7, S7 based Servers component of Oracle Sun Systems Products Suite (subcomponent: Firmware). The	http://www.oracle.com/technetwork	A-ORA-SPARC-011117/262

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			supported version that is affected is Prior to 9.7.6.b. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where SPARC M7, T7, S7 based Servers Executeutes to compromise SPARC M7, T7, S7 based Servers. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of SPARC M7, T7, S7 based Servers. CVSS 3.0 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2017-10099**	/security-advisory/cpuoct2017-3236626.html	
Trade Management					
NA	19-10-2017	5.8	Vulnerability in the Oracle Trade Management component of Oracle E-Business Suite (subcomponent: User Interface). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5 and 12.2.6. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Trade Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Trade Management, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Trade Management accessible data as well as unauthorized update, insert or delete access to some of Oracle Trade Management accessible	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-TRADE-011117/263

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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
			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-2017-3446**		
NA	19-10-2017	5.8	Vulnerability in the Oracle Trade Management component of Oracle E-Business Suite (subcomponent: User Interface). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5 and 12.2.6. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Trade Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Trade Management, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Trade Management accessible data as well as unauthorized update, insert or delete access to some of Oracle Trade Management accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N). **CVE ID : CVE-2017-3445**	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-TRADE-011117/264
NA	19-10-2017	5.8	Vulnerability in the Oracle Trade Management component of Oracle E-Business Suite (subcomponent: User Interface). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5 and 12.2.6. Easily exploitable vulnerability allows	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-	A-ORA-TRADE-011117/265

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 Oracle Trade Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Trade Management, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Trade Management accessible data as well as unauthorized update, insert or delete access to some of Oracle Trade Management accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N). **CVE ID : CVE-2017-3444**	3236626.html	
Universal Work Queue					
Gain Information	19-10-2017	5	Vulnerability in the Oracle Universal Work Queue component of Oracle E-Business Suite (subcomponent: Administration). 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 Universal Work Queue. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Universal Work Queue accessible data. CVSS 3.0 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-UNIVE-011117/266

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			S:U/C:H/I:N/A:N). **CVE ID : CVE-2017-10332**		
Virtual Directory					
NA	19-10-2017	6	Vulnerability in the Oracle Virtual Directory component of Oracle Fusion Middleware (subcomponent: Virtual Directory Server). Supported versions that are affected are 11.1.1.7.0 and 11.1.1.9.0. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Virtual Directory. Successful attacks of this vulnerability can result in takeover of Oracle Virtual Directory. CVSS 3.0 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H). **CVE ID : CVE-2017-10369**	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-VIRTU-011117/267
Vm Virtualbox					
DoS	19-10-2017	4.1	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). The supported version that is affected is Prior to 5.1.30. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox Executeutes 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 unauthorized update, insert or delete access to some of Oracle VM VirtualBox accessible data as well as unauthorized read access to a subset of Oracle VM VirtualBox accessible data and unauthorized ability to cause a partial denial of	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-VMVI-011117/268

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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
			service (partial DOS) of Oracle VM VirtualBox. CVSS 3.0 Base Score 5.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:L/I:L/A:L). **CVE ID : CVE-2017-10428**		
NA	19-10-2017	4.3	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). The supported version that is affected is Prior to 5.1.30. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox Executeutes 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 unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox as well as unauthorized update, insert or delete access to some of Oracle VM VirtualBox accessible data and unauthorized read access to a subset of Oracle VM VirtualBox accessible data. CVSS 3.0 Base Score 7.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/C:L/I:L/A:H). **CVE ID : CVE-2017-10408**	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-VM VI-011117/269
NA	19-10-2017	4.3	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). The supported version that is affected is Prior to 5.1.30. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-	A-ORA-VM VI-011117/270

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			VM VirtualBox Executeutes 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 unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox as well as unauthorized update, insert or delete access to some of Oracle VM VirtualBox accessible data and unauthorized read access to a subset of Oracle VM VirtualBox accessible data. CVSS 3.0 Base Score 7.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/C:L/I:L/A:H). **CVE ID : CVE-2017-10407**	3236626.html	
NA	19-10-2017	4.3	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). The supported version that is affected is Prior to 5.1.30. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox Executeutes 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 unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox as well as unauthorized update, insert or delete access to some of Oracle VM VirtualBox accessible data and unauthorized read access to a	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-VM VI-011117/271

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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
			subset of Oracle VM VirtualBox accessible data. CVSS 3.0 Base Score 7.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/C:L/I:L/A:H). **CVE ID : CVE-2017-10392**		
Web Applications Desktop Integrator					
NA	19-10-2017	5.8	Vulnerability in the Oracle Web Applications Desktop Integrator component of Oracle E-Business Suite (subcomponent: Application Service). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5 and 12.2.6. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Web Applications Desktop Integrator. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Web Applications Desktop Integrator, 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 Web Applications Desktop Integrator accessible data as well as unauthorized update, insert or delete access to some of Oracle Web Applications Desktop Integrator 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-2017-10323**	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-WEB A-011117/272
Webcenter Content					
NA	19-10-2017	5.8	Vulnerability in the Oracle	http://w	A-ORA-

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			WebCenter Content component of Oracle Fusion Middleware (subcomponent: Content Server). Supported versions that are affected are 11.1.1.9.0, 12.2.1.1.0 and 12.2.1.2.0. 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-2017-10360**	ww.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	WEBCE-011117/273
Webcenter Sites					
NA	19-10-2017	3.3	Vulnerability in the Oracle WebCenter Sites component of Oracle Fusion Middleware (subcomponent: Support Tools). Supported versions that are affected are 11.1.1.8.0 and 12.2.1.2.0. Difficult to exploit vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle WebCenter Sites Executeutes to compromise Oracle WebCenter Sites. Successful attacks of this vulnerability can result in unauthorized update,	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-WEBCE-011117/274

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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
			insert or delete access to some of Oracle WebCenter Sites accessible data as well as unauthorized read access to a subset of Oracle WebCenter Sites accessible data. Note: Please refer to Doc ID <a href="http://support.oracle.com/CSP/main/article?cmd=show&type=NOT&id=2318213.1">My Oracle Support Note 2318213.1 for instructions on how to address this issue. CVSS 3.0 Base Score 4.0 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N). **CVE ID : CVE-2017-10033**		
Weblogic Server					
Gain Information	19-10-2017	4	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: Web Container). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.1.0 and 12.2.1.2.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle WebLogic Server accessible data. CVSS 3.0 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2017-10334**	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-WEBLO-011117/275
Gain Information	19-10-2017	4	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: Web Container). Supported versions that are affected are 10.3.6.0.0 and 12.1.3.0.0. Easily exploitable	http://www.oracle.com/technetwork/security-advisory/cpuoct20	A-ORA-WEBLO-011117/276

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server 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-2017-10152**	17-3236626.html	
NA	19-10-2017	4.3	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: WLS-WebServices). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.1.0 and 12.2.1.2.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle WebLogic Server. CVSS 3.0 Base Score 5.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2017-10352**	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-WEBLO-011117/277
NA	19-10-2017	5	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: Web Container). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.1.0 and 12.2.1.2.0. Easily exploitable vulnerability allows unauthenticated attacker with	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.	A-ORA-WEBLO-011117/278

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 WebLogic Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle WebLogic Server accessible data. CVSS 3.0 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2017-10336**	html	
NA	19-10-2017	7.5	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: WLS Security). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.1.0 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 takeover of Oracle WebLogic Server. CVSS 3.0 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H). **CVE ID : CVE-2017-10271**	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	A-ORA-WEBLO-011117/279
Paessler					
Prtg Network Monitor					
Execute Code	19-10-2017	6.5	PRTG Network Monitor 17.3.33.2830 allows remote authenticated administrators to Execute arbitrary code by uploading a .exe file and then proceeding in spite of the error message. **CVE ID : CVE-2017-15651**	https://medium.com/stolabs/security-issue-on-prtg-network-manager-ada65b45d37b	A-PAE-PRTG - 011117/280
Phpjabbers					
Rate Me					

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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
XSS	16-10-2017	4.3	rate-me.php in Rate Me 1.0 has XSS via the id field in a rate action. **CVE ID : CVE-2017-15384**	NA	A-PHP-RATE - 011117/ 281
Phpmyfaq					
Phpmyfaq					
XSS	22-10-2017	3.5	In phpMyFAQ before 2.9.9, there is Stored Cross-site Scripting (XSS) via metaDescription or metaKeywords. **CVE ID : CVE-2017-15728**	https://github.com/thorsten/phpMyFAQ/commit/2d2a85b59e058869d7cbcfe2d73fed4a282f2e5b	A-PHP-PHPMY-011117/ 282
XSS	22-10-2017	4.3	In phpMyFAQ before 2.9.9, there is Stored Cross-site Scripting (XSS) via an HTML attachment. **CVE ID : CVE-2017-15727**	https://github.com/thorsten/phpMyFAQ/commit/5c3e4f96ff0ef6b91a3f0aa64eb28197c5cf5435	A-PHP-PHPMY-011117/ 283
XSS	23-10-2017	4.3	In phpMyFaq before 2.9.9, there is XSS in admin/tags.main.php via a crafted tag. **CVE ID : CVE-2017-15809**	https://github.com/thorsten/phpMyFAQ/commit/cb648f0d5690b81647dd5c9efe942ebf6cce7da9	A-PHP-PHPMY-011117/284
CSRF	22-10-2017	6.8	In phpMyFAQ before 2.9.9, there is Cross-Site Request Forgery (CSRF) for modifying a glossary. **CVE ID : CVE-2017-15735**	https://github.com/thorsten/phpMyFAQ/commit/867618110feb	A-PHP-PHPMY-011117/ 285

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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
				836e168435548d6c2cbb7c65eda3	
CSRF	22-10-2017	6.8	In phpMyFAQ before 2.9.9, there is Cross-Site Request Forgery (CSRF) in admin/stat.main.php. **CVE ID : CVE-2017-15734**	https://github.com/thorsten/phpMyFAQ/commit/fa26c52384b010edaf60c525ae5b040f05da9f77	A-PHP-PHPMY-011117/286
CSRF	22-10-2017	6.8	In phpMyFAQ before 2.9.9, there is Cross-Site Request Forgery (CSRF) in admin/ajax.attachment.php and admin/att.main.php. **CVE ID : CVE-2017-15733**	https://github.com/thorsten/phpMyFAQ/commit/ef5a66df4bcfacc7573322af33ce10c30e0bb896	A-PHP-PHPMY-011117/287
CSRF	22-10-2017	6.8	In phpMyFAQ before 2.9.9, there is Cross-Site Request Forgery (CSRF) in admin/news.php. **CVE ID :CVE-2017-15732**	https://github.com/thorsten/phpMyFAQ/commit/ec8b3cc37d05b6625e24916b8f7253f830015b5f	A-PHP-PHPMY-011117/288
CSRF	22-10-2017	6.8	In phpMyFAQ before 2.9.9, there is Cross-Site Request Forgery (CSRF) in admin/stat.adminlog.php. **CVE ID : CVE-2017-15731**	https://github.com/thorsten/phpMyFAQ/commit/fadb9a70b5f7624a6926b8834d5c	A-PHP-PHPMY-011117/289

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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
				6001c210f09c	
CSRF	22-10-2017	6.8	In phpMyFAQ before 2.9.9, there is Cross-Site Request Forgery (CSRF) in admin/stat.ratings.php. **CVE ID : CVE-2017-15730**	https://github.com/thorsten/phpMyFAQ/commit/cce47f94375bb0102ab4f210672231dbb854dd0d	A-PHP-PHPMY-011117/290
CSRF	22-10-2017	6.8	In phpMyFAQ before 2.9.9, there is Cross-Site Request Forgery (CSRF) for adding a glossary. **CVE ID : CVE-2017-15729**	https://github.com/thorsten/phpMyFAQ/commit/867618110febb836e168435548d6c2cbb7c65eda3	A-PHP-PHPMY-011117/291
CSRF	23-10-2017	6.8	In phpMyFaq before 2.9.9, there is CSRF in admin/ajax.config.php. **CVE ID : CVE-2017-15808**	https://github.com/thorsten/phpMyFAQ/commit/a249b4645fb86f6a9fbe5d2344ab1cbdb906b75c	A-PHP-PHPMY-011117/292
Phpwcms					
Phpwcms					
XSS	24-10-2017	3.5	phpwcms 1.8.9 has XSS in include/inc_tmpl/admin.edituser.tmpl.php and include/inc_tmpl/admin.newuser.tmpl.php via the username (aka new_login) field. **CVE ID : CVE-2017-15872**	https://github.com/slackero/phpwcms/commit/90ee94a474b37919161f8112f9e36c	A-PHP-PHPWC-011117/293

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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
				53ad70492f	
Post Highlights Projects					
Post Highlights					
XSS	16-10-2017	4.3	Cross-site scripting (XSS) vulnerability in the post highlights plugin before 2.6.1 for WordPress allows remote attackers to inject arbitrary web script or HTML via the txt parameter in a headline action to ajax/ph_save.php. **CVE ID : CVE-2014-8087**	https://wordpress.org/plugins/post-highlights/#developers	A-POS-POST - 011117/294
Qemu					
Qemu					
DoS	16-10-2017	2.1	The mode4and5 write functions in hw/display/cirrus_vga.c in Qemu allow local OS guest privileged users to cause a denial of service (out-of-bounds write access and Qemu process crash) via vectors related to dst calculation. **CVE ID : CVE-2017-15289**	https://bugzilla.redhat.com/show_bug.cgi?id=1501290	A-QEM-QEMU-011117/295
Radare					
Radare2					
DoS Overflow	16-10-2017	6.8	The store_versioninfo_gnu_verdef function in libr/bin/format/elf/elf.c in radare2 2.0.0 allows remote attackers to cause a denial of service (r_read_le16 invalid write and application crash) or possibly have unspecified other impact via a crafted ELF file. **CVE ID : CVE-2017-15385**	https://github.com/radare/radare2/issues/8685	A-RAD-RADAR-011117/296
NA	27-10-2017	6.8	In radare2 2.0.1, an integer exception (negative number leading to an invalid memory access) exists in store_versioninfo_gnu_verdef() in libr/bin/format/elf/elf.c via crafted ELF files when parsing the ELF version on 32bit systems. **CVE ID : CVE-2017-15932**	https://github.com/radare/radare2/commit/44ded3ff35b8264f54b5a900cab32ec489d9e5b9	A-RAD-RADAR-011117/297
NA	27-10-2017	6.8	In radare2 2.0.1, an integer	https://gi	A-RAD-

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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
			exception (negative number leading to an invalid memory access) exists in store_versioninfo_gnu_verneed() in libr/bin/format/elf/elf.c via crafted ELF files on 32bit systems. **CVE ID : CVE-2017-15931**	thub.com/radare/radare2/commit/c6d0076c924891ad9948a62d89d0bcdaf965f0cd	RADAR-011117/298
Redmine					
Redmine					
XSS	17-10-2017	4.3	In Redmine before 3.2.6 and 3.3.x before 3.3.3, stored XSS is possible by using an SVG document as an attachment. **CVE ID : CVE-2017-15574**	https://www.redmine.org/issues/24199	A-RED-REDMI-011117/299
XSS	17-10-2017	4.3	In Redmine before 3.2.6 and 3.3.x before 3.3.3, XSS exists because markup is mishandled in wiki content. **CVE ID : CVE-2017-15573**	https://www.redmine.org/issues/25503	A-RED-REDMI-011117/300
XSS	17-10-2017	4.3	In Redmine before 3.2.8, 3.3.x before 3.3.5, and 3.4.x before 3.4.3, XSS exists in app/views/issues/_list.html.erb via crafted column data. **CVE ID : CVE-2017-15571**	https://www.redmine.org/projects/redmine/wiki/Security_Advisories	A-RED-REDMI-011117/301
XSS	17-10-2017	4.3	In Redmine before 3.2.8, 3.3.x before 3.3.5, and 3.4.x before 3.4.3, XSS exists in app/views/timelog/_list.html.erb via crafted column data. **CVE ID : CVE-2017-15570**	https://www.redmine.org/projects/redmine/wiki/Security_Advisories	A-RED-REDMI-011117/302
XSS	17-10-2017	4.3	In Redmine before 3.2.8, 3.3.x before 3.3.5, and 3.4.x before 3.4.3, XSS exists in app/helpers/queries_helper.rb via a multi-value field with a crafted value that is mishandled during rendering of an issue list. **CVE ID : CVE-2017-15569**	https://www.redmine.org/projects/redmine/wiki/Security_Advisories	A-RED-REDMI-011117/303
XSS	17-10-2017	4.3	In Redmine before 3.2.8, 3.3.x	https://gi	A-RED-

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			before 3.3.5, and 3.4.x before 3.4.3, XSS exists in app/helpers/application_helper.rb via a multi-value field with a crafted value that is mishandled during rendering of issue history. **CVE ID : CVE-2017-15568**	thub.com/redmine/redmine/commit/94f7cfbf99002834 8b9262578acbc53a94fce448	REDMI-011117/304
XSS	17-10-2017	4.3	In Redmine before 3.2.3, there are stored XSS vulnerabilities affecting Textile and Markdown text formatting, and project homepages. **CVE ID : CVE-2016-10515**	https://www.redmine.org/projects/redmine/wiki/Security_Advisories	A-RED-REDMI-011117/305
Gain Information	17-10-2017	5	Redmine before 3.2.6 and 3.3.x before 3.3.3 mishandles the rendering of wiki links, which allows remote attackers to obtain sensitive information. **CVE ID : CVE-2017-15577**	https://www.redmine.org/issues/23793	A-RED-REDMI-011117/306
Gain Information	17-10-2017	5	Redmine before 3.2.6 and 3.3.x before 3.3.3 mishandles Time Entry rendering in activity views, which allows remote attackers to obtain sensitive information. **CVE ID : CVE-2017-15576**	https://www.redmine.org/issues/23803	A-RED-REDMI-011117/307
Gain Information	17-10-2017	5	In Redmine before 3.2.6 and 3.3.x before 3.3.3, remote attackers can obtain sensitive information (password reset tokens) by reading a Referer log, because account/lost_password does not use a redirect. **CVE ID : CVE-2017-15572**	https://www.redmine.org/issues/24416	A-RED-REDMI-011117/308
Gain Information	17-10-2017	7.5	In Redmine before 3.2.6 and 3.3.x before 3.3.3, Redmine.pm lacks a check for whether the Repository module is enabled in a project's settings, which might allow remote attackers to obtain sensitive differences information or possibly have unspecified other	https://www.redmine.org/issues/24307	A-RED-REDMI-011117/309

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			impact. **CVE ID : CVE-2017-15575**		
SAP					
Customer Relationship Management					
XSS	16-10-2017	4.3	The Java administration console in SAP CRM has XSS. This is SAP Security Note 2478964. **CVE ID : CVE-2017-15294**	NA	A-SAP-CUSTO-011117/310
CSRF	16-10-2017	6.8	The Java component in SAP CRM has CSRF. This is SAP Security Note 2478964. **CVE ID : CVE-2017-15296**	NA	A-SAP-CUSTO-011117/311
Softwarepublico					
E-sic					
XSS	23-10-2017	4.3	XSS exists in the E-Sic 1.0 /cadastro/index.php URI (aka the requester's registration area) via the nome parameter. **CVE ID : CVE-2017-15380**	NA	A-SOF-E-SIC-011117/312
Sql	23-10-2017	6.5	SQL Injection exists in the E-Sic 1.0 password reset parameter (aka the cpfcnpj parameter to the /reset URI). **CVE ID : CVE-2017-15378**	NA	A-SOF-E-SIC-011117/313
Sql	16-10-2017	7.5	E-Sic 1.0 allows SQL injection via the q parameter to esiclivre/restrito/inc/lkpcep.php (aka the search private area). **CVE ID : CVE-2017-15373**	NA	A-SOF-E-SIC-011117/314
Sql	23-10-2017	7.5	SQL Injection exists in E-Sic 1.0 via the f parameter to esiclivre/restrito/inc/buscacep.php (aka the zip code search script). **CVE ID : CVE-2017-15381**	https://www.exploit-db.com/exploits/42982/	A-SOF-E-SIC-011117/315
Soundexchange					
Sound Exchange					
DoS Overflow	16-10-2017	4.3	There is a stack-based buffer overflow in the lsx_ms_adpcm_block_expand_i function of adpcm.c in Sound eXchange (SoX) 14.4.2. A Crafted input will lead to a denial of service attack during conversion of an audio file.	https://bugzilla.redhat.com/show_bug.cgi?id=1500553	A-SOU-SOUND-011117/316

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2017-15372		
DoS Overflow	16-10-2017	4.3	There is a reachable assertion abort in the function sox_append_comment() in formats.c in Sound eXchange (SoX) 14.4.2. A Crafted input will lead to a denial of service attack during conversion of an audio file. **CVE ID : CVE-2017-15371**	https://bugzilla.redhat.com/show_bug.cgi?id=1500570	A-SOU-SOUND-011117/317
DoS Overflow	16-10-2017	4.3	There is a heap-based buffer overflow in the ImaExpandS function of ima_rw.c in Sound eXchange (SoX) 14.4.2. A Crafted input will lead to a denial of service attack during conversion of an audio file. **CVE ID : CVE-2017-15370**	https://bugzilla.redhat.com/show_bug.cgi?id=1500554	A-SOU-SOUND-011117/318
NA	19-10-2017	4.3	In lsx_aiffstartread in aiff.c in Sound eXchange (SoX) 14.4.2, there is a Use-After-Free vulnerability triggered by supplying a malformed AIFF file. **CVE ID : CVE-2017-15642**	https://sourceforge.net/p/sox/bugs/298/	A-SOU-SOUND-011117/319
Store Locator Project					
Store Locator					
Execute Code Sql	16-10-2017	7.5	SQL injection vulnerability in the Store Locator plugin 2.3 through 3.11 for WordPress allows remote attackers to Executeute arbitrary SQL commands via the sl_custom_field parameter to sl-xml.php. **CVE ID : CVE-2014-8621**	NA	A-STO-STORE-011117/320
Theforeman					
Foreman					
XSS	18-10-2017	3.5	Multiple cross-site scripting (XSS) vulnerabilities in Foreman before 1.5.2 allow remote authenticated users to inject arbitrary web script or HTML via the operating system (1) name or (2) description. **CVE ID : CVE-2014-3531**	https://github.com/theforeman/foreman/pull/1580	A-THE-FOREM-011117/321
Web2py					
Web2py					
NA	18-10-2017	5.8	Open redirect vulnerability in	https://gi	A-WEB-

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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
			gluon/tools.py in Web2py 2.9.11 allows remote attackers to redirect users to arbitrary web sites and conduct phishing attacks via a URL in the _next parameter to user/logout. **CVE ID : CVE-2015-6961**	thub.com /web2py /web2py /issues/7 31	WEB2P-011117/ 322
WPA;Wpa2					
WPA/Wpa2					
NA	16-10-2017	5.4	Wi-Fi Protected Access (WPA and WPA2) allows reinstallation of the Pairwise Transient Key (PTK) Temporal Key (TK) during the four-way handshake, allowing an attacker within radio range to replay, decrypt, or spoof frames. **CVE ID : CVE-2017-13077**	https://access.redhat.com/security/vulnerabilities/kracks	A-WPA-WPA/W-011117/ 323
Xnview					
Xnview					
DoS Overflow	22-10-2017	6.8	XnView Classic for Windows Version 2.43 allows attackers to cause a denial of service or possibly have unspecified other impact via a crafted .dll file that is mishandled during an attempt to render the DLL icon, related to "Data from Faulting Address is used as one or more arguments in a subsequent Function Call starting at ntdll_77310000!LdrpResCompareResourceNames+0x0000000000000150." **CVE ID : CVE-2017-15803**	https://github.com/wlinzi/security_advisories/tree/master/CVE-2017-15803	A-XNV-XNVIE-011117/ 324
DoS Overflow	22-10-2017	6.8	XnView Classic for Windows Version 2.43 allows attackers to cause a denial of service or possibly have unspecified other impact via a crafted .dll file that is mishandled during an attempt to render the DLL icon, related to "Data from Faulting Address controls Branch Selection starting at ntdll_77310000!LdrpResCompareResourceNames+0x00000000000	https://github.com/wlinzi/security_advisories/tree/master/CVE-2017-15802	A-XNV-XNVIE-011117/ 325

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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
			00087." **CVE ID : CVE-2017-15802**		
DoS Overflow	22-10-2017	6.8	XnView Classic for Windows Version 2.43 allows attackers to cause a denial of service or possibly have unspecified other impact via a crafted .dll file that is mishandled during an attempt to render the DLL icon, related to "Data from Faulting Address controls Branch Selection starting at ntdll_77310000!LdrpResSearchResourceInsideDirectory+0x000000000000029e." **CVE ID : CVE-2017-15801**	https://github.com/wlinzi/security_advisories/tree/master/CVE-2017-15801	A-XNV-XNVIE-011117/326
DoS Execute Code Overflow	22-10-2017	6.8	XnView Classic for Windows Version 2.43 allows attackers to Execute arbitrary code or cause a denial of service via a crafted .dwg file, related to a "User Mode Write AV starting at CADImage+0x00000000000048e7." **CVE ID : CVE-2017-15789**	https://github.com/wlinzi/security_advisories/tree/master/CVE-2017-15789	A-XNV-XNVIE-011117/327
DoS Execute Code Overflow	22-10-2017	6.8	XnView Classic for Windows Version 2.43 allows attackers to Execute arbitrary code or cause a denial of service via a crafted .dwg file, related to a "User Mode Write AV starting at CADImage+0x0000000000002d83." **CVE ID : CVE-2017-15788**	https://github.com/wlinzi/security_advisories/tree/master/CVE-2017-15788	A-XNV-XNVIE-011117/328
DoS Execute Code Overflow	22-10-2017	6.8	XnView Classic for Windows Version 2.43 allows attackers to Execute arbitrary code or cause a denial of service via a crafted .dwg file, related to a "Data Executeution Prevention Violation starting at xnview+0x0000000000580063." **CVE ID : CVE-2017-15787**	https://github.com/wlinzi/security_advisories/tree/master/CVE-2017-15787	A-XNV-XNVIE-011117/329
DoS Overflow	22-10-2017	6.8	XnView Classic for Windows Version 2.43 allows attackers to cause a denial of service or	https://github.com/wlinzi/s	A-XNV-XNVIE-011117/

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			possibly have unspecified other impact via a crafted .dwg file, related to a "Read Access Violation starting at CADImage+0x00000000001a78db ." **CVE ID : CVE-2017-15786**	ecurity_advisories/tree/master/CVE-2017-15786	330
DoS Execute Code Overflow	22-10-2017	6.8	XnView Classic for Windows Version 2.43 allows attackers to Execute arbitrary code or cause a denial of service via a crafted .dwg file, related to a "Data Execution Prevention Violation near NULL starting at Unknown Symbol @ 0x0000000000000000 called from CADImage+0x0000000000286a79 ."**CVE ID : CVE-2017-15785**	https://github.com/wlinzi/security_advisories/tree/master/CVE-2017-15785	A-XNV-XNVIE-011117/331
DoS Execute Code Overflow	22-10-2017	6.8	XnView Classic for Windows Version 2.43 allows attackers to Execute arbitrary code or cause a denial of service via a crafted .dwg file, related to an "Illegal Instruction Violation starting at xnview+0x0000000000370074." **CVE ID : CVE-2017-15784**	https://github.com/wlinzi/security_advisories/tree/master/CVE-2017-15784	A-XNV-XNVIE-011117/332
DoS Overflow	22-10-2017	6.8	XnView Classic for Windows Version 2.43 allows attackers to cause a denial of service or possibly have unspecified other impact via a crafted .dwg file, related to "Data from Faulting Address controls Branch Selection starting at CADImage+0x0000000000285ce1 ." **CVE ID : CVE-2017-15783**	https://github.com/wlinzi/security_advisories/tree/master/CVE-2017-15783	A-XNV-XNVIE-011117/333
DoS Execute Code Overflow	22-10-2017	6.8	XnView Classic for Windows Version 2.43 allows attackers to Execute arbitrary code or cause a denial of service via a crafted .dwg file, related to a "User Mode Write AV starting at CADImage+0x00000000000032eb ."**CVE ID : CVE-2017-15782**	https://github.com/wlinzi/security_advisories/tree/master/CVE-2017-15782	A-XNV-XNVIE-011117/334
DoS Execute	22-10-2017	6.8	XnView Classic for Windows	https://gi	A-XNV-

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Code Overflow			Version 2.43 allows attackers to Execute arbitrary code or cause a denial of service via a crafted .dwg file, related to a "Read Access Violation on Control Flow starting at CADImage+0x0000000000286a76 ." **CVE ID : CVE-2017-15781**	thub.com /wlinzi/security_advisories /tree/master/CVE-2017-15781	XNVIE-011117/335
DoS Overflow	22-10-2017	6.8	XnView Classic for Windows Version 2.43 allows attackers to cause a denial of service or possibly have unspecified other impact via a crafted .dwg file, related to a "Read Access Violation starting at CADImage+0x0000000000285dad ." **CVE ID : CVE-2017-15780**	https://github.com/wlinzi/security_advisories/tree/master/CVE-2017-15780	A-XNV-XNVIE-011117/336
DoS Execute Code Overflow	22-10-2017	6.8	XnView Classic for Windows Version 2.43 allows attackers to Execute arbitrary code or cause a denial of service via a crafted .dwg file, related to "Data from Faulting Address controls subsequent Write Address starting at CADImage+0x00000000000034b0 ." **CVE ID : CVE-2017-15779**	https://github.com/wlinzi/security_advisories/tree/master/CVE-2017-15779	A-XNV-XNVIE-011117/337
DoS Overflow	22-10-2017	6.8	XnView Classic for Windows Version 2.43 allows attackers to cause a denial of service or possibly have unspecified other impact via a crafted .dwg file, related to a "Read Access Violation starting at CADImage+0x0000000000285de7 ." **CVE ID : CVE-2017-15778**	https://github.com/wlinzi/security_advisories/tree/master/CVE-2017-15778	A-XNV-XNVIE-011117/338
DoS Execute Code Overflow	22-10-2017	6.8	XnView Classic for Windows Version 2.43 allows attackers to Execute arbitrary code or cause a denial of service via a crafted .dwg file, related to a "User Mode Write AV near NULL starting at CADImage+0x0000000000288750 ." **CVE ID : CVE-2017-15777**	https://github.com/wlinzi/security_advisories/tree/master/CVE-2017-15777	A-XNV-XNVIE-011117/339
DoS Overflow	22-10-2017	6.8	XnView Classic for Windows Version 2.43 allows attackers to	https://github.com	A-XNV-XNVIE-

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service or possibly have unspecified other impact via a crafted .dwg file, related to "Data from Faulting Address may be used as a return value starting at CADImage+0x0000000000285ec1 ." **CVE ID : CVE-2017-15776**	/wlinzi/security_advisories/tree/master/CVE-2017-15776	011117/340
DoS Overflow	22-10-2017	6.8	XnView Classic for Windows Version 2.43 allows attackers to cause a denial of service or possibly have unspecified other impact via a crafted .dwg file, related to "Data from Faulting Address controls Branch Selection starting at CADImage+0x0000000000259aa4 ." **CVE ID : CVE-2017-15775**	https://github.com/wlinzi/security_advisories/tree/master/CVE-2017-15775	A-XNV-XNVIE-011117/341
DoS Execute Code Overflow	22-10-2017	6.8	XnView Classic for Windows Version 2.43 allows attackers to Execute arbitrary code or cause a denial of service via a crafted .dwg file, related to "Data from Faulting Address controls Code Flow starting at CADImage+0x0000000000221a9a ." **CVE ID : CVE-2017-15774**	https://github.com/wlinzi/security_advisories/tree/master/CVE-2017-15774	A-XNV-XNVIE-011117/342
DoS Overflow	22-10-2017	6.8	XnView Classic for Windows Version 2.43 allows attackers to cause a denial of service or possibly have unspecified other impact via a crafted .dwg file, related to a "Read Access Violation starting at CADImage+0x0000000000285d79 ." **CVE ID : CVE-2017-15773**	https://github.com/wlinzi/security_advisories/tree/master/CVE-2017-15773	A-XNV-XNVIE-011117/343
DoS Overflow	22-10-2017	6.8	XnView Classic for Windows Version 2.43 allows attackers to cause a denial of service or possibly have unspecified other impact via a crafted .dwg file, related to "Data from Faulting Address may be used as a return value starting at CADImage+0x0000000000285e9d ." **CVE ID : CVE-2017-15772**	https://github.com/wlinzi/security_advisories/tree/master/CVE-2017-15772	A-XNV-XNVIE-011117/344

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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
Application;OS(A/OS)					
Apple/Apple					
Apple Tv/Iphone Os					
DoS Execute Code Mem. Corr.	22-10-2017	9.3	An issue was discovered in certain Apple products. iOS before 11 is affected. tvOS before 11 is affected. The issue involves the "Wi-Fi" component. It might allow remote attackers to Execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via crafted Wi-Fi traffic that leverages a race condition. **CVE ID : CVE-2017-7115**	https://support.apple.com/HT208112	A-APP-APPLE-011117/345
Apple Tv/Iphone Os;Mac Os X;Watchos					
DoS	22-10-2017	4	An issue was discovered in certain Apple products. iOS before 11 is affected. macOS before 10.13 is affected. tvOS before 11 is affected. watchOS before 4 is affected. The issue involves the "CFNetwork Proxies" component. It allows remote attackers to cause a denial of service. **CVE ID : CVE-2017-7083**	https://support.apple.com/HT208144	A-APP-APPLE-011117/346
Bypass	22-10-2017	5	An issue was discovered in certain Apple products. iOS before 11 is affected. macOS before 10.13 is affected. tvOS before 11 is affected. watchOS before 4 is affected. The issue involves the "Security" component. It allows remote attackers to bypass intended certificate-trust restrictions via a revoked X.509 certificate. **CVE ID : CVE-2017-7080**	https://support.apple.com/HT208144	A-APP-APPLE-011117/347
DoS Overflow	22-10-2017	7.5	An issue was discovered in certain Apple products. iOS before 11 is affected. macOS before 10.13 is affected. tvOS before 11 is affected. watchOS before 4 is affected. The issue involves the third-party "SQLite" product. Versions before 3.19.3 allow remote attackers to cause a denial of service	https://support.apple.com/HT208144	A-APP-APPLE-011117/348

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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
			(application crash) or possibly have unspecified other impact.**CVE ID : CVE-2017-7130**		
DoS Overflow	22-10-2017	7.5	An issue was discovered in certain Apple products. iOS before 11 is affected. macOS before 10.13 is affected. tvOS before 11 is affected. watchOS before 4 is affected. The issue involves the third-party "SQLite" product. Versions before 3.19.3 allow remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact.**CVE ID : CVE-2017-7129**	https://support.apple.com/HT208144	A-APP-APPLE-011117/349
DoS Overflow	22-10-2017	7.5	An issue was discovered in certain Apple products. iOS before 11 is affected. macOS before 10.13 is affected. tvOS before 11 is affected. watchOS before 4 is affected. The issue involves the third-party "SQLite" product. Versions before 3.19.3 allow remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact.**CVE ID : CVE-2017-7128**	https://support.apple.com/HT208144	A-APP-APPLE-011117/350
DoS	22-10-2017	7.8	An issue was discovered in certain Apple products. iOS before 11 is affected. macOS before 10.13 is affected. tvOS before 11 is affected. watchOS before 4 is affected. The issue involves the "libc" component. It allows remote attackers to cause a denial of service (resource consumption) via a crafted string that is mishandled by the glob function. **CVE ID : CVE-2017-7086**	https://support.apple.com/HT208144	A-APP-APPLE-011117/351
DoS Execute Code Overflow Mem. Corr.	22-10-2017	9.3	An issue was discovered in certain Apple products. iOS before 11 is affected. macOS before 10.13 is affected. tvOS before 11 is affected. watchOS before 4 is affected. The issue involves the "Kernel" component. It allows attackers to	https://support.apple.com/HT208144	A-APP-APPLE-011117/352

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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
			Executeute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app. **CVE ID : CVE-2017-7114**		
Apple Tv/Iphone Os;Watchos					
Gain Information	22-10-2017	5	An issue was discovered in certain Apple products. iOS before 11 is affected. tvOS before 11 is affected. watchOS before 4 is affected. The issue involves the "Wi-Fi" component. It might allow remote attackers to read data from kernel memory locations via crafted Wi-Fi traffic. **CVE ID : CVE-2017-7116**	https://support.apple.com/HT208115	A-APP-APPLE-011117/353
DoS Execute Code Overflow Mem. Corr.	22-10-2017	7.5	An issue was discovered in certain Apple products. iOS before 11 is affected. tvOS before 11 is affected. watchOS before 4 is affected. The issue involves the "Wi-Fi" component. It might allow remote attackers to Execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via crafted Wi-Fi traffic. **CVE ID : CVE-2017-7103**	https://support.apple.com/HT208115	A-APP-APPLE-011117/354
DoS Execute Code Overflow Mem. Corr.	22-10-2017	10	An issue was discovered in certain Apple products. iOS before 11 is affected. tvOS before 11 is affected. watchOS before 4 is affected. The issue involves the "Wi-Fi" component. It might allow remote attackers to Execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via crafted Wi-Fi traffic. **CVE ID : CVE-2017-7112**	https://support.apple.com/HT208115	A-APP-APPLE-011117/355
DoS Execute Code Overflow Mem. Corr.	22-10-2017	10	An issue was discovered in certain Apple products. iOS before 11 is affected. tvOS before 11 is affected. watchOS before 4 is affected. The issue involves the "Wi-Fi" component. It might allow remote	https://support.apple.com/HT208115	A-APP-APPLE-011117/356

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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
			attackers to Execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via crafted Wi-Fi traffic. **CVE ID : CVE-2017-7110**		
DoS Execute Code Overflow Mem. Corr.	22-10-2017	10	An issue was discovered in certain Apple products. iOS before 11 is affected. tvOS before 11 is affected. watchOS before 4 is affected. The issue involves the "Wi-Fi" component. It might allow remote attackers to Execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via crafted Wi-Fi traffic. **CVE ID : CVE-2017-7108**	https://support.apple.com/HT208115	A-APP-APPLE-011117/357
DoS Execute Code Overflow Mem. Corr.	22-10-2017	10	An issue was discovered in certain Apple products. iOS before 11 is affected. tvOS before 11 is affected. watchOS before 4 is affected. The issue involves the "Wi-Fi" component. It might allow remote attackers to Execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via crafted Wi-Fi traffic. **CVE ID : CVE-2017-7105**	https://support.apple.com/HT208115	A-APP-APPLE-011117/358
Apple Tv;Icloud/Iphone Os;Mac Os X;Watchos					
DoS Execute Code Overflow Mem. Corr.	22-10-2017	9.3	An issue was discovered in certain Apple products. iOS before 11 is affected. macOS before 10.13 is affected. iCloud before 7.0 on Windows is affected. tvOS before 11 is affected. watchOS before 4 is affected. The issue involves the "SQLite" component. It allows attackers to Execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app. **CVE ID : CVE-2017-7127**	https://support.apple.com/HT208144	A-APP-APPLE-011117/359
Apple Tv;Icloud;Itunes;Safari/Iphone Os					
XSS	22-10-2017	4.3	An issue was discovered in certain	https://s	A-APP-

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Apple products. iOS before 11 is affected. Safari before 11 is affected. iCloud before 7.0 on Windows is affected. iTunes before 12.7 on Windows is affected. tvOS before 11 is affected. The issue involves the "WebKit" component. A cross-site scripting (XSS) vulnerability allows remote attackers to inject arbitrary web script or HTML via crafted web content that incorrectly interacts with the Application Cache policy. **CVE ID : CVE-2017-7109**	upport.apple.com/HT208142	APPLE-011117/360
XSS	22-10-2017	4.3	An issue was discovered in certain Apple products. iOS before 11 is affected. Safari before 11 is affected. iCloud before 7.0 on Windows is affected. The issue involves the "WebKit" component. It allows remote attackers to conduct Universal XSS (UXSS) attacks via a crafted web site that is mishandled during parent-tab processing. **CVE ID : CVE-2017-7089**	https://support.apple.com/HT208142	A-APP-APPLE-011117/361
Bypass Gain Information	22-10-2017	5	An issue was discovered in certain Apple products. iOS before 11 is affected. Safari before 11 is affected. iCloud before 7.0 on Windows is affected. iTunes before 12.7 on Windows is affected. tvOS before 11 is affected. The issue involves the "WebKit" component. It allows remote attackers to bypass the Same Origin Policy and obtain sensitive cookie information via a custom URL scheme. **CVE ID : CVE-2017-7090**	https://support.apple.com/HT208142	A-APP-APPLE-011117/362
DoS Execute Code Overflow Mem. Corr.	22-10-2017	6.8	An issue was discovered in certain Apple products. iOS before 11 is affected. Safari before 11 is affected. iCloud before 7.0 on Windows is affected. iTunes before 12.7 on Windows is affected. tvOS	https://support.apple.com/HT208142	A-APP-APPLE-011117/363

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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
			before 11 is affected. The issue involves the "WebKit" component. It allows remote attackers to Execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site. **CVE ID : CVE-2017-7120**		
DoS Execute Code Overflow Mem. Corr.	22-10-2017	6.8	An issue was discovered in certain Apple products. iOS before 11 is affected. Safari before 11 is affected. iCloud before 7.0 on Windows is affected. iTunes before 12.7 on Windows is affected. tvOS before 11 is affected. The issue involves the "WebKit" component. It allows remote attackers to Executeute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site. **CVE ID : CVE-2017-7117**	https://support.apple.com/HT208113	A-APP-APPLE-011117/364
DoS Execute Code Overflow Mem. Corr.	22-10-2017	6.8	An issue was discovered in certain Apple products. iOS before 11 is affected. Safari before 11 is affected. iCloud before 7.0 on Windows is affected. iTunes before 12.7 on Windows is affected. tvOS before 11 is affected. The issue involves the "WebKit" component. It allows remote attackers to Execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site. **CVE ID : CVE-2017-7111**	https://support.apple.com/HT208142	A-APP-APPLE-011117/365
DoS Execute Code Overflow Mem. Corr.	22-10-2017	6.8	An issue was discovered in certain Apple products. iOS before 11 is affected. Safari before 11 is affected. iCloud before 7.0 on Windows is affected. iTunes before 12.7 on Windows is affected. tvOS before 11 is affected. The issue involves the "WebKit" component. It allows remote attackers to Execute arbitrary code or cause a	https://support.apple.com/HT208142	A-APP-APPLE-011117/366

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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
			denial of service (memory corruption and application crash) via a crafted web site. **CVE ID : CVE-2017-7107**		
DoS Execute Code Overflow Mem. Corr.	22-10-2017	6.8	An issue was discovered in certain Apple products. iOS before 11 is affected. Safari before 11 is affected. iCloud before 7.0 on Windows is affected. iTunes before 12.7 on Windows is affected. tvOS before 11 is affected. The issue involves the "WebKit" component. It allows remote attackers to Execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site. **CVE ID : CVE-2017-7104**	https://support.apple.com/HT208142	A-APP-APPLE-011117/367
DoS Execute Code Overflow Mem. Corr.	22-10-2017	6.8	An issue was discovered in certain Apple products. iOS before 11 is affected. Safari before 11 is affected. iCloud before 7.0 on Windows is affected. iTunes before 12.7 on Windows is affected. tvOS before 11 is affected. The issue involves the "WebKit" component. It allows remote attackers to Execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.**CVE ID: CVE-2017-7102**	https://support.apple.com/HT208142	A-APP-APPLE-011117/368
DoS Execute Code Overflow Mem. Corr.	22-10-2017	6.8	An issue was discovered in certain Apple products. iOS before 11 is affected. Safari before 11 is affected. iCloud before 7.0 on Windows is affected. iTunes before 12.7 on Windows is affected. tvOS before 11 is affected. The issue involves the "WebKit" component. It allows remote attackers to Execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.**CVE ID: CVE-2017-7100**	https://support.apple.com/HT208142	A-APP-APPLE-011117/369

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
DoS Execute Code Overflow Mem. Corr.	22-10-2017	6.8	An issue was discovered in certain Apple products. iOS before 11 is affected. Safari before 11 is affected. iCloud before 7.0 on Windows is affected. iTunes before 12.7 on Windows is affected. tvOS before 11 is affected. The issue involves the "WebKit" component. It allows remote attackers to Execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.**CVE ID: CVE-2017-7099**	https://support.apple.com/HT208142	A-APP-APPLE-011117/370
DoS Execute Code Overflow Mem. Corr.	22-10-2017	6.8	An issue was discovered in certain Apple products. iOS before 11 is affected. Safari before 11 is affected. iCloud before 7.0 on Windows is affected. iTunes before 12.7 on Windows is affected. tvOS before 11 is affected. The issue involves the "WebKit" component. It allows remote attackers to Execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.**CVE ID: CVE-2017-7098**	https://support.apple.com/HT208142	A-APP-APPLE-011117/371
DoS Execute Code Overflow Mem. Corr.	22-10-2017	6.8	An issue was discovered in certain Apple products. iOS before 11 is affected. Safari before 11 is affected. iCloud before 7.0 on Windows is affected. iTunes before 12.7 on Windows is affected. tvOS before 11 is affected. The issue involves the "WebKit" component. It allows remote attackers to Execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.**CVE ID : CVE-2017-7096**	https://support.apple.com/HT208142	A-APP-APPLE-011117/372
DoS Execute Code Overflow Mem. Corr.	22-10-2017	6.8	An issue was discovered in certain Apple products. iOS before 11 is affected. Safari before 11 is affected. iCloud before 7.0 on	https://support.apple.com/HT20814	A-APP-APPLE-011117/373

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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
			Windows is affected. iTunes before 12.7 on Windows is affected. tvOS before 11 is affected. The issue involves the "WebKit" component. It allows remote attackers to Execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.**CVE ID: CVE-2017-7095**	2	
DoS Execute Code Overflow Mem. Corr.	22-10-2017	6.8	An issue was discovered in certain Apple products. iOS before 11 is affected. Safari before 11 is affected. iCloud before 7.0 on Windows is affected. iTunes before 12.7 on Windows is affected. tvOS before 11 is affected. The issue involves the "WebKit" component. It allows remote attackers to Execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.**CVE ID: CVE-2017-7094**	https://support.apple.com/HT208142	A-APP-APPLE-011117/374
DoS Execute Code Overflow Mem. Corr.	22-10-2017	6.8	An issue was discovered in certain Apple products. iOS before 11 is affected. Safari before 11 is affected. iCloud before 7.0 on Windows is affected. iTunes before 12.7 on Windows is affected. tvOS before 11 is affected. The issue involves the "WebKit" component. It allows remote attackers to Execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.**CVE ID: CVE-2017-7093**	https://support.apple.com/HT208142	A-APP-APPLE-011117/375
DoS Execute Code Overflow Mem. Corr.	22-10-2017	6.8	An issue was discovered in certain Apple products. iOS before 11 is affected. Safari before 11 is affected. iCloud before 7.0 on Windows is affected. iTunes before 12.7 on Windows is affected. tvOS before 11 is affected. The issue involves the "WebKit" component.	https://support.apple.com/HT208142	A-APP-APPLE-011117/376

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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
			It allows remote attackers to Executeute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.**CVE ID :CVE-2017-7092**		
DoS Execute Code Overflow Mem. Corr.	22-10-2017	6.8	An issue was discovered in certain Apple products. iOS before 11 is affected. Safari before 11 is affected. iCloud before 7.0 on Windows is affected. iTunes before 12.7 on Windows is affected. tvOS before 11 is affected. The issue involves the "WebKit" component. It allows remote attackers to Execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.**CVE ID :CVE-2017-7091**	https://support.apple.com/HT208142	A-APP-APPLE-011117/377
DoS Execute Code Overflow Mem. Corr.	22-10-2017	6.8	An issue was discovered in certain Apple products. iOS before 11 is affected. Safari before 11 is affected. iCloud before 7.0 on Windows is affected. iTunes before 12.7 on Windows is affected. tvOS before 11 is affected. The issue involves the "WebKit" component. It allows remote attackers to Execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.**CVE ID :CVE-2017-7087**	https://support.apple.com/HT208142	A-APP-APPLE-011117/378
DoS Execute Code Overflow Mem. Corr.	22-10-2017	6.8	An issue was discovered in certain Apple products. iOS before 11 is affected. Safari before 11 is affected. iCloud before 7.0 on Windows is affected. iTunes before 12.7 on Windows is affected. tvOS before 11 is affected. The issue involves the "WebKit" component. It allows remote attackers to Execute arbitrary code or cause a denial of service (memory corruption and application crash)	https://support.apple.com/HT208142	A-APP-APPLE-011117/379

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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
			via a crafted web site.**CVE ID :CVE-2017-7081**		
Icloud;Safari/Iphone Os					
NA	22-10-2017	4.3	An issue was discovered in certain Apple products. iOS before 11 is affected. Safari before 11 is affected. iCloud before 7.0 on Windows is affected. The issue involves the "WebKit" component. It allows remote attackers to spoof the address bar. **CVE ID : CVE-2017-7106**	https://support.apple.com/HT208142	A-APP-ICLOU-011117/380
Qemu/XEN					
Qemu/XEN					
DoS Execute Code Overflow	16-10-2017	4.6	Heap-based buffer overflow in the pcnet_receive function in hw/net/pcnet.c in QEMU allows guest OS administrators to cause a denial of service (instance crash) or possibly Execute arbitrary code via a series of packets in loopback mode. **CVE ID : CVE-2015-7504**	http://xenbits.xen.org/xsa/advisory-162.html	A-QEM-QEMU/-011117/381
OPERATING SYSTEM(OS)					
Apple					
Iphone Os					
Gain Information	22-10-2017	2.1	An issue was discovered in certain Apple products. iOS before 11 is affected. The issue involves the "Phone" component. It allows attackers to obtain sensitive information by leveraging a timing bug to read a secure-content screenshot that occurred during a locking action. **CVE ID : CVE-2017-7139**	https://support.apple.com/HT208112	O-APP-IPHON-011117/382
Gain Information	22-10-2017	4.3	An issue was discovered in certain Apple products. iOS before 11 is affected. The issue involves the "Location Framework" component. It allows attackers to obtain sensitive location information via a crafted app that reads the location variable. **CVE ID : CVE-2017-7148**	https://support.apple.com/HT208112	O-APP-IPHON-011117/383

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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	22-10-2017	4.3	An issue was discovered in certain Apple products. iOS before 11 is affected. The issue involves the "Bluetooth" component. It allows attackers to obtain sensitive Contact card information via a crafted app. **CVE ID : CVE-2017-7131**	https://support.apple.com/HT208112	O-APP-IPHON-011117/384
DoS	22-10-2017	4.3	An issue was discovered in certain Apple products. iOS before 11 is affected. The issue involves the "Messages" component. It allows remote attackers to cause a denial of service (crash) via a crafted image.**CVE ID : CVE-2017-7118**	https://support.apple.com/HT208112	O-APP-IPHON-011117/385
DoS Overflow Mem. Corr.	22-10-2017	4.3	An issue was discovered in certain Apple products. iOS before 11 is affected. The issue involves the "Mail MessageUI" component. It allows attackers to cause a denial of service (memory corruption) via a crafted image. **CVE ID : CVE-2017-7097**	https://support.apple.com/HT208112	O-APP-IPHON-011117/386
DoS	22-10-2017	4.3	An issue was discovered in certain Apple products. iOS before 11 is affected. The issue involves the "iBooks" component. It allows remote attackers to cause a denial of service (persistent outage) via a crafted iBooks file. **CVE ID : CVE-2017-7072**	https://support.apple.com/HT208112	O-APP-IPHON-011117/387
NA	22-10-2017	5	An issue was discovered in certain Apple products. iOS before 11 is affected. The issue involves the "Security" component. It allows attackers to track users across installs via a crafted app that leverages Keychain data mishandling. **CVE ID : CVE-2017-7146**	https://support.apple.com/HT208112	O-APP-IPHON-011117/388
NA	22-10-2017	5	An issue was discovered in certain Apple products. iOS before 11 is affected. The issue involves the "Time" component. The "Setting Time Zone" feature mishandles the possibility of using location	https://support.apple.com/HT208112	O-APP-IPHON-011117/389

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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
			data.**CVE ID : CVE-2017-7145**		
Gain Information	22-10-2017	5	An issue was discovered in certain Apple products. iOS before 11 is affected. The issue involves the "Keyboard Suggestions" component. It allows attackers to obtain sensitive information by reading keyboard autocorrect suggestions. **CVE ID : CVE-2017-7140**	https://support.apple.com/HT208112	O-APP-IPHON-011117/390
Gain Information	22-10-2017	5	An issue was discovered in certain Apple products. iOS before 11 is affected. The issue involves the "MobileBackup" component. It allows remote attackers to obtain sensitive cleartext information in opportunistic circumstances by leveraging read access to a backup archive that was supposed to have been encrypted. **CVE ID : CVE-2017-7133**	https://support.apple.com/HT208112	O-APP-IPHON-011117/391
NA	22-10-2017	7.1	An issue was discovered in certain Apple products. iOS before 11 is affected. The issue involves the "Exchange ActiveSync" component. It allows remote attackers to erase a device in opportunistic circumstances by hijacking a cleartext AutoDiscover V1 session during the setup of an Exchange account. **CVE ID : CVE-2017-7088**	https://support.apple.com/HT208112	O-APP-IPHON-011117/392
Iphone Os;Mac Os X					
Gain Information	22-10-2017	5	An issue was discovered in certain Apple products. iOS before 11 is affected. macOS before 10.13 is affected. The issue involves the "Mail Drafts" component. It allows remote attackers to obtain sensitive information by reading unintended cleartext transmissions. **CVE ID : CVE-2017-7078**	https://support.apple.com/HT208144	O-APP-IPHON-011117/393
Mac Os X					
Bypass	22-10-2017	2.1	An issue was discovered in certain Apple products. macOS before	https://support.ap	O-APP-MAC O-

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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
			10.13 Supplemental Update is affected. The issue involves the "Security" component. It allows attackers to bypass the keychain access prompt, and consequently extract passwords, via a synthetic click.**CVE ID : CVE-2017-7150**	ple.com/HT208165	011117/394
Gain Information	22-10-2017	2.1	An issue was discovered in certain Apple products. macOS before 10.13 Supplemental Update is affected. The issue involves the "StorageKit" component. It allows attackers to discover passwords for APFS encrypted volumes by reading Disk Utility hints, because the stored hint value was accidentally set to the password itself, not the entered hint value.**CVE ID : CVE-2017-7149**	https://support.apple.com/HT208165	O-APP-MAC O-011117/395
Gain Information	22-10-2017	2.1	An issue was discovered in certain Apple products. macOS before 10.13 is affected. The issue involves the "Captive Network Assistant" component. It allows remote attackers to discover cleartext passwords in opportunistic circumstances by sniffing the network during use of the captive portal browser, which has a UI error that can lead to cleartext transmission without the user's awareness. **CVE ID : CVE-2017-7143**	https://support.apple.com/HT208144	O-APP-MAC O-011117/396
Gain Information	22-10-2017	2.1	An issue was discovered in certain Apple products. macOS before 10.13 is affected. The issue involves the "Directory Utility" component. It allows local users to discover the Apple ID of the computer's owner. **CVE ID : CVE-2017-7138**	https://support.apple.com/HT208144	O-APP-MAC O-011117/397
Gain Information	22-10-2017	2.1	An issue was discovered in certain Apple products. macOS before 10.13 is affected. The issue involves the "Screen Lock" component. It allows physically	https://support.apple.com/HT208144	O-APP-MAC O-011117/398

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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
			proximate attackers to read Application Firewall prompts. **CVE ID : CVE-2017-7082**		
Bypass	22-10-2017	4.3	An issue was discovered in certain Apple products. macOS before 10.13 is affected. The issue involves the "IOFireWireFamily" component. It allows attackers to bypass intended memory-read restrictions via a crafted app. **CVE ID : CVE-2017-7119**	https://support.apple.com/HT208144	O-APP-MAC O-011117/399
Bypass	22-10-2017	4.3	An issue was discovered in certain Apple products. macOS before 10.13 is affected. The issue involves the "Application Firewall" component. It allows remote attackers to bypass intended settings in opportunistic circumstances by leveraging incorrect handling of a denied setting after an upgrade. **CVE ID : CVE-2017-7084**	https://support.apple.com/HT208144	O-APP-MAC O-011117/400
DoS	22-10-2017	4.3	An issue was discovered in certain Apple products. macOS before 10.13 is affected. The issue involves the "AppSandbox" component. It allows attackers to cause a denial of service via a crafted app. **CVE ID : CVE-2017-7074**	https://support.apple.com/HT208144	O-APP-MAC O-011117/401
Bypass Gain Information	22-10-2017	5	An issue was discovered in certain Apple products. macOS before 10.13 is affected. The issue involves the "Mail" component. It allows remote attackers to bypass an intended off value of the "Load remote content in messages" setting, and consequently discover an e-mail recipient's IP address, via an HTML email message. **CVE ID : CVE-2017-7141**	https://support.apple.com/HT208144	O-APP-MAC O-011117/402
DoS Execute Code Overflow Mem. Corr.	22-10-2017	6.8	An issue was discovered in certain Apple products. Xcode before 9 is affected. The issue involves the "ld64" component. It allows remote attackers to Execute	https://support.apple.com/HT208103	O-APP-MAC O-011117/403

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted Mach-O file. **CVE ID : CVE-2017-7076**		
DoS	22-10-2017	7.5	An issue was discovered in certain Apple products. macOS before 10.13 is affected. The issue involves the third-party "file" product. Versions before 5.30 allow remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact. **CVE ID : CVE-2017-7126**	https://support.apple.com/HT208144	O-APP-MAC O-011117/404
DoS	22-10-2017	7.5	An issue was discovered in certain Apple products. macOS before 10.13 is affected. The issue involves the third-party "file" product. Versions before 5.30 allow remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact. **CVE ID : CVE-2017-7125**	https://support.apple.com/HT208144	O-APP-MAC O-011117/405
DoS	22-10-2017	7.5	An issue was discovered in certain Apple products. macOS before 10.13 is affected. The issue involves the third-party "file" product. Versions before 5.30 allow remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact. **CVE ID : CVE-2017-7124**	https://support.apple.com/HT208144	O-APP-MAC O-011117/406
DoS	22-10-2017	7.5	An issue was discovered in certain Apple products. macOS before 10.13 is affected. The issue involves the third-party "file" product. Versions before 5.30 allow remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact. **CVE ID : CVE-2017-7123**	https://support.apple.com/HT208144	O-APP-MAC O-011117/407
DoS	22-10-2017	7.5	An issue was discovered in certain	https://s	O-APP-

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Apple products. macOS before 10.13 is affected. The issue involves the third-party "file" product. Versions before 5.30 allow remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact. **CVE ID : CVE-2017-7122**	upport.apple.com/HT208144	MAC O-011117/408
DoS	22-10-2017	7.5	An issue was discovered in certain Apple products. macOS before 10.13 is affected. The issue involves the third-party "file" product. Versions before 5.30 allow remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact. **CVE ID : CVE-2017-7121**	https://support.apple.com/HT208144	O-APP-MAC O-011117/409
DoS Execute Code Overflow Mem. Corr.	22-10-2017	9.3	An issue was discovered in certain Apple products. macOS before 10.13 is affected. The issue involves the "IOFireWireFamily" component. It allows attackers to Executeute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app. **CVE ID : CVE-2017-7077**	https://support.apple.com/HT208144	O-APP-MAC O-011117/410
Fortinet					
Fortios					
DoS	27-10-2017	4	A Denial of Service (DoS) vulnerability in Fortinet FortiOS 5.4.0 to 5.4.5 allows an authenticated user to cause the web GUI to be temporarily unresponsive, via passing a specially crafted payload to the 'params' parameter of the JSON web API. **CVE ID : CVE-2017-14182**	https://fortiguard.com/psirt/FG-IR-17-206	O-FOR-FORTI-011117/411
Execute Code XSS	27-10-2017	4.3	A Cross-Site-Scripting (XSS) vulnerability in Fortinet FortiOS 5.4.0 to 5.4.5 and 5.6.0 allows a remote unauthenticated attacker to Executeute arbitrary javascript	https://fortiguard.com/psirt/FG-IR-17-113	O-FOR-FORTI-011117/412

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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
			code via webUI "Login Disclaimer" redir parameter. **CVE ID : CVE-2017-7733**		
Linux					
Linux Kernel					
DoS	16-10-2017	6.9	Race condition in the ALSA subsystem in the Linux kernel before 4.13.8 allows local users to cause a denial of service (use-after-free) or possibly have unspecified other impact via crafted /dev/snd/seq ioctl calls, related to sound/core/seq/seq_clientmgr.c and sound/core/seq/seq_ports.c. **CVE ID : CVE-2017-15265**	http://www.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.13.8	O-LIN-LINUX-011117/413
Oracle					
Integrated Lights Out Manager Firmware					
Gain Information	19-10-2017	4	Vulnerability in the Oracle Integrated Lights Out Manager (ILOM) component of Oracle Sun Systems Products Suite (subcomponent: System Management). The supported version that is affected is Prior to 3.2.6. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Integrated Lights Out Manager (ILOM). Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Integrated Lights Out Manager (ILOM) accessible data. CVSS 3.0 Base Score 2.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2017-10194**	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	O-ORA-INTEG-011117/414
DoS	19-10-2017	7.5	Vulnerability in the Oracle Integrated Lights Out Manager (ILOM) component of Oracle Sun Systems Products Suite (subcomponent: System	http://www.oracle.com/technetwork/security-	O-ORA-INTEG-011117/415

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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
			Management). The supported version that is affected is Prior to 3.2.6. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Integrated Lights Out Manager (ILOM). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Integrated Lights Out Manager (ILOM) accessible data as well as unauthorized read access to a subset of Oracle Integrated Lights Out Manager (ILOM) accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Integrated Lights Out Manager (ILOM). CVSS 3.0 Base Score 7.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L). **CVE ID : CVE-2017-10265**	advisory/cpuoct2017-3236626.html	
NA	19-10-2017	7.8	Vulnerability in the Oracle Integrated Lights Out Manager (ILOM) component of Oracle Sun Systems Products Suite (subcomponent: System Management). The supported version that is affected is Prior to 3.2.6. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Integrated Lights Out Manager (ILOM). Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Integrated Lights Out Manager	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	O-ORA-INTEG-011117/416

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(ILOM). 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-2017-10260**		
Solaris Ak					
NA	19-10-2017	6.3	Vulnerability in the Sun ZFS Storage Appliance Kit (AK) component of Oracle Sun Systems Products Suite (subcomponent: Filesystem). The supported version that is affected is AK 2013. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Sun ZFS Storage Appliance Kit (AK) Execute to compromise Sun ZFS Storage Appliance Kit (AK). 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 hang or frequently repeatable crash (complete DOS) of Sun ZFS Storage Appliance Kit (AK). CVSS 3.0 Base Score 5.0 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:H). **CVE ID : CVE-2017-10275**	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html	O-ORA-SOLAR-011117/417
XEN					
XEN					
DoS Gain Privileges	18-10-2017	4.6	An issue was discovered in Xen through 4.9.x allowing x86 SVM PV guest OS users to cause a denial of service (hypervisor crash) or gain privileges because IDT settings are mishandled during CPU hotplugging. **CVE ID : CVE-2017-15594**	https://xenbits.xen.org/xsa/advisory-244.html	O-XEN-XEN-011117/418
DoS Gain Privileges	18-10-2017	4.6	An issue was discovered in Xen through 4.9.x allowing x86 guest OS users to cause a denial of	https://xenbits.xen.org/xsa/	O-XEN-XEN-011117/

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			service (hypervisor crash) or possibly gain privileges because MSI mapping was mishandled. **CVE ID : CVE-2017-15590**	advisory-237.html	419
DoS	18-10-2017	4.9	An issue was discovered in Xen 4.4.x through 4.9.x allowing ARM guest OS users to cause a denial of service (prevent physical CPU usage) because of lock mishandling upon detection of an add-to-physmap error. **CVE ID : CVE-2017-15596**	https://xenbits.xen.org/xsa/advisory-235.html	O-XEN-XEN-011117/420
DoS Overflow	18-10-2017	4.9	An issue was discovered in Xen through 4.9.x allowing x86 PV guest OS users to cause a denial of service (memory leak) because reference counts are mishandled. **CVE ID : CVE-2017-15593**	https://xenbits.xen.org/xsa/advisory-242.html	O-XEN-XEN-011117/421
DoS	18-10-2017	4.9	An issue was discovered in Xen 4.5.x through 4.9.x allowing attackers (who control a stub domain kernel or tool stack) to cause a denial of service (host OS crash) because of a missing comparison (of range start to range end) within the DMOP map/unmap implementation. **CVE ID : CVE-2017-15591**	https://xenbits.xen.org/xsa/advisory-238.html	O-XEN-XEN-011117/422
DoS Gain Privileges	18-10-2017	7.2	An issue was discovered in Xen through 4.9.x allowing x86 PV guest OS users to cause a denial of service (unbounded recursion, stack consumption, and hypervisor crash) or possibly gain privileges via crafted page-table stacking. **CVE ID : CVE-2017-15595**	https://xenbits.xen.org/xsa/advisory-240.html	O-XEN-XEN-011117/423
DoS Gain Privileges	18-10-2017	7.2	An issue was discovered in Xen through 4.9.x allowing x86 HVM guest OS users to cause a denial of service (hypervisor crash) or possibly gain privileges because self-linear shadow mappings are mishandled for translated guests. **CVE ID : CVE-2017-15592**	https://xenbits.xen.org/xsa/advisory-243.html	O-XEN-XEN-011117/424

OS;Application (OS/A)

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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
Apple/Apple					
Iphone Os/Safari					
NA	22-10-2017	4.3	An issue was discovered in certain Apple products. iOS before 11 is affected. Safari before 11 is affected. The issue involves the "WebKit" component. It allows remote attackers to track Safari Private Browsing users by leveraging cookie mishandling. **CVE ID : CVE-2017-7144**	https://support.apple.com/HT208116	O-APP-IPHON-011117/425
NA	22-10-2017	4.3	An issue was discovered in certain Apple products. iOS before 11 is affected. Safari before 11 is affected. The issue involves the "Safari" component. It allows remote attackers to spoof the address bar. **CVE ID : CVE-2017-7085**	https://support.apple.com/HT208116	O-APP-IPHON-011117/426

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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;