	National C	ritical	Information Infrastructure Pr CVE Report 16-31 Oct 2017	rotection Centre Vol. 04 No.18			
Vulnerability	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID		
Type(s)	Date		Application (A)				
Apache			Application (A)				
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.or g/derby/ releases/ release- 10.6.2.1.h tml#Note +for+DER BY-2925	A-APA- DERBY- 011117/1		
Apple				21 27 20			
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://s upport.ap ple.com/ HT20820 1	A-APP- APPLE- 011117/2		
<u>Itunes</u> 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://s upport.ap ple.com/ HT20814 0	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://s upport.ap ple.com/	A-APP- SAFAR- 011117/4		
CV Scoring Scale (C	VSS)	0-1	1-2 2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10		
Vulnerability Type CSRF-Cross Site Rec Injection; XSS- Cros	uest Forgery; Dir	. TravDir	rectory Traversal; DoS-Denial of Service; NA- N	ot Applicable; S	ql-SQL		

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	HT20811 6	
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://s upport.ap ple.com/ HT20810 3	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://s upport.ap ple.com/ HT20810 3	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://s upport.ap ple.com/ HT20810 3	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://s upport.ap ple.com/ HT20810 3	A-APP- XCODE- 011117/8
CV Scoring Scale (CV	VSS)	0-1	1-2 2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10
Vulnerability Type(CSRF-Cross Site Reg	uest Forgery; Dir	. TravDir	ectory Traversal; DoS-Denial of Service; NA- N	ot Applicable; S	ql-SQL

Busyboxstartfinal ghostghostori ghostori pdf/pdf-xref.c in Artifex MuPDF int.11.ghostori pt.com/?p final cVE ID : CVE-2017-15587final ghostBusyboxCVE ID : CVE-2017-15587631d7d0 446b206e a6b434ea 609b6c28 b0e8Busyboxnlma.c in BusyBox 1.27.2 has an integer Underflow that leads to a read access violation. CVE ID : CVE-2017-15874https://b gi?id=104 36Overflow24-10-20174.3Archival/libarchive/decompress_u nlma.c in BusyBox 1.27.2 has an integer Underflow that leads to a read access violation. CVE ID : CVE-2017-15874with access violation. gi?id=104 36jOverflow24-10-20174.3The get_next_block function in archival/libarchive/decompress_b unzip2.c in BusyBox 1.27.2 has an in BusyBox 1.27.2 has an integer Overflow that may lead to a write access violation. CVE ID : CVE-2017-15873jFfmpegCVE ID : CVE-2017-158731j	A-ART- MUPDF- 011117/9
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. http://git.f ///ghtextef.c in Artifex MuPDF 1.11. CVE ID : CVE-2017-15587 631d7d0 446b206e a6b434ea 609b6c28 b0e8 Busybox nlzma.c in BusyBox 1.27.2 has an Integer Underflow that leads to a read access violation. https://b // git.id=104 36 Overflow 24-10-2017 4.3 The get_next_block function in archival/libarchive/decompress_b unzip2.c in BusyBox 1.27.2 has an Integer Underflow that leads to a read access violation. NA 24-10-2017 4.3 Floppeg Underflow 12 - 10 - 2017 4.3 The get_next_block function in archival/libarchive/decompress_b unzip2.c in BusyBox 1.27.2 has an Integer Overflow that may lead to a write access violation. NA 24-10 - 2017 4.3 Floppeg Underflow 12 - 10 - 2017 4.3 The get_next_block function in archival/libarchive/decompress_b unzip2.c in BusyBox 1.27.2 has an Integer Overflow that may lead to a write access violation. 12 - 10 - 2017	MUPDF-)11117/9
MupdfOverflow18-10-20176.8An integer overflow was discovered in pdf_read_new_xref_section in pt.com/?p for pdf/pdf-xref.c in Artifex MuPDF in pdf/pdf-xref.c in Artifex MuPDF in the sector is pt.com/?p for the sector is pt.com/?p for pdf/pdf-xref.c in Artifex MuPDF in the sector is pt.com/?p for pdf/pdf-xref.c in Artifex MuPDF in the sector is pt.com/?p for pdf/pdf-xref.c in Artifex MuPDF in the sector is pt.com/?p for pdf/pdf-xref.c in Artifex MuPDF in the sector is pt.com/?p for pdf/pdf-xref.c in Artifex MuPDF in the sector is pt.com/?p for pdf/pdf-xref.c in Artifex MuPDF in the sector is pt.com/?p for pdf/pdf-xref.c in Artifex MuPDF in the sector is pt.com/?p for pdf/pdf-xref.c in Artifex MuPDF in the sector is pt.com/?p for pdf/pdf-xref.c in Artifex MuPDF in the sector is pt.com/?p for pdf/pdf-xref.c in Artifex MuPDF in the sector is pt.com/?p for pdf/pdf-xref.c in Artifex MuPDF in the sector is pt.com/?p for pdf/pdf-xref.c in Artifex MuPDF in the sector is pt.com/?p for pdf/pdf-xref.c in Artifex MuPDF in the sector is pt.com/?p for pdf/pdf-xref.c in Artifex MuPDF in the sector is pt.com/?p for pdf/pdf-xref.c in Artifex MuPDF in the sector is pt.com/?p for pdf/pdf-xref.c in Artifex MuPDF in the sector is pt.com/?p for pdf/pdf-xref.c in Artifex MuPDF in the sector is pt.com/?p for pdf/pdf-xref.c in Artifex MuPDF in the sector is pt.com/?p for pdf/pdf-xref.c in the sector is pt.com/?p for pdf/pdf-xref.com/?p for pdf-xref.com/?p for pdf-xref.com/?p for pdf-xref.com/?p for pdf-xref.com/?p for pd	MUPDF-)11117/9
Overflow18-10-20176.8An integer overflow was discovered in pdf_read_new_xref_section in pdf/pdf-xref.c in Artifex MuPDF 1.11. CVE ID : CVE-2017-15587http://git. / ghostscri in pt.com/?pBusyboxBusyboxBusyboxNA24-10-20174.3 archival/libarchive/decompress_u nlteger Underflow that leads to a read access violation. CVE ID : CVE-2017-15874https://b 	MUPDF-)11117/9
BusyboxHttps://bABusyboxarchival/libarchive/decompress_u nlmeger Underflow that leads to a read access violation.https://bAOverflow24-10-20174.3archival/libarchive/decompress_u nlmeger Underflow that leads to a 	MUPDF-)11117/9
BusyboxNA24-10-20174.3archival/libarchive/decompress_u nlzma.c in BusyBox 1.27.2 has an Integer Underflow that leads to a read access violation. 	
NA24-10-20174.3archival/libarchive/decompress_uhttps://b//nlzma.c in BusyBox 1.27.2 has anugs.busybHnlzma.c in BusyBox 1.27.2 has anugs.busybHInteger Underflow that leads to aox.net/sh0read access violation.ow_bug.c1Overflow24-10-20174.3The get_next_block function in archival/libarchive/decompress_bNAOverflow24-10-20174.3The get_next_block function in narchival/libarchive/decompress_bInteger Overflow that may lead to a write access violation.Integer Overflow that may lead to a write access violation.1FfmpegFfmpegFfmpegFfmpegFfmpegFfmpeg	
Overflow24-10-20174.3The get_next_block function in archival/libarchive/decompress_b unzip2.c in BusyBox 1.27.2 has an icead access violation. CVE ID : CVE-2017-15874Ugs.busyb ox.net/shH o ow_bug.c gi?id=104 36Overflow24-10-20174.3The get_next_block function in archival/libarchive/decompress_b unzip2.c in BusyBox 1.27.2 has an integer Overflow that may lead to a write access violation. CVE ID : CVE-2017-15873NAA J 	
archival/libarchive/decompress_b H unzip2.c in BusyBox 1.27.2 has an 0 Integer Overflow that may lead to 1 a write access violation. 1 CVE ID : CVE-2017-15873 1 Ffmpeg 1	A-BUS- BUSYB- D11117/ LO
Ffmpeg	A-BUS- BUSYB- D11117/ L1
FFmpeg 3.3.4 and earlier allows FFmpeg 3.3.4 and earlier allows FFmpeg 3.3.4 and earlier allows FFmpeg 4.3.4 and earlier allows 4.3.4 and earlier allows 4.3.4 and earlier allows 4.3.4 and earlier allows 4.3.4 and earlier a	A-FFM- FFMPE-)11117/ 12
Fiyo	
Fiyo Cms	
Informationattackers to obtain sensitiveHinformation via a direct request to0	A-FIY- FIYO -)11117/ 13
Bypass 16-10-2017 7.5 Fiyo CMS 2.0.1.8 allows remote NA A	
CV Scoring Scale (CVSS) 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8	A-FIY- FIYO -
Vulnerability Type(s):	

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 <i>Flexpaper</i>							
XSS	17-10-2017	4.3	Cross-sitescripting(XSS)NAvulnerabilityinFlexPaperViewer.swf in Flexpaperbefore2.3.1allowsremoteattackers to inject arbitrary webscript or HTML via the Swfileparameter.CVE ID : CVE-2014-9677	A-FLO- FLEXP- 011117/ 15			
Foxitsoftware							
Foxit Reader							
DoS Execute Code Overflow	22-10-2017	6.8	Foxit Reader 8.3.2.25013 allows NA 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+0x000000000 000158." CVE ID : CVE-2017- 15771	A-FOX- FOXIT- 011117/ 16			
Foxit Reader							
DoS Execute Code Overflow	22-10-2017	6.8	Foxit Reader 8.3.2.25013 allowsNAattackers to Execute arbitrarycode or cause a denial of servicevia a crafted .xps file, related to"Data from Faulting Addresscontrols subsequent WriteAddress starting atfrdvpr_drv!DrvQueryDriverInfo+0x0000000002c851."CVE ID : CVE-2017-15770	A-FOX- FOXIT- 011117/ 17			
Freedesktop							
Poppler NA	17-10-2017	6.8	In Poppler 0.59.0, a NULL Pointerhttps://bDereferenceexistsintheGfxImageColorMap::getGrayLine()esktop.onfunction in GfxState.cc via a craftedg/show_l	POPPL- 011117/			
CV Scoring Scale (C	VSS)	0-1	1-2 2-3 3-4 4-5 5-6 6-7 7-8	8-9 9-10			
or scoring scale (C							

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
	Dute		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	NA	A-GNU- BINUT- 011117/
			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		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://s ourcewar e.org/bug zilla/sho w_bug.cgi ?id=2232 5	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://s ourcewar e.org/bug zilla/sho	A-GNU- GLIBC- 011117/ 22
CV Scoring Scale (CV	VSS)	0-1	1-2 2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10
Vulnerability Type((s): quest Forgery; Dir	. TravDir	ectory Traversal; DoS-Denial of Service; NA- N	lot Applicable; S	Sql-SQL

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=2232 0	
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://s ourcewar e.org/bug zilla/sho w_bug.cgi ?id=2233 2	A-GNU- GLIBC- 011117/ 23
Libextractor	<u> </u>				
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
Graphicsmagic					
Graphicsmagic NA	k 27-10-2017	6.8	In PondOnoINCImago in	https://a	A-GRA-
	27-10-2017	0.0	In ReadOneJNGImage in coders/png.c in GraphicsMagick 1.3.26, a Null Pointer Dereference	https://s ourceforg e.net/p/g	GRAPH- 011117/
CV Scoring Scale (C	VSS)	0-1	1-2 2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10
Vulnerability Type CSRF-Cross Site Rec Injection; XSS- Cros	quest Forgery; Dir	. TravDir	ectory Traversal; DoS-Denial of Service; NA- N	ot Applicable; S	ql-SQL

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE IDPatchNCIIPC ID
			occurs while transferring JPEGraphicsm28scanlines, related to a PixelPacketagick/bugpointer.s/518/CVE ID : CVE-2017-15930
IBM			
Bigfix Platform Gain Information	26-10-2017	4	IBM Tivoli Endpoint Manager (IBMhttp://wA-IBM-BigFix Platform 9.2 and 9.5)ww.ibm.cBIGFI-generates an error message inom/supp011117/error logs that includes sensitiveort/docvi29information about its environmentew.wss?uiwhich could be used in furtherd=swg22attacks against the system. IBM X-009673Force ID: 123905.Key EndCVE ID : CVE-2017-1226Key End
XSS	26-10-2017	4.3	IBM Tivoli Endpoint Manager (for Lifecycle/Power/Patch)http://w Platform ww.ibm.cA-IBM- BIGFI- 011117/ 30and Applications (IBM BigFix Platform 9.2 and 9.5) is vulnerable to cross-site scripting. This wulnerability allows users to to d=swg22 embed arbitrary JavaScript code in the Web UI thus altering the
Gain Information	26-10-2017	4.3	IBM Tivoli Endpoint Manager (IBMhttp://wA-IBM-BigFix Platform 9.2 and 9.5)ww.ibm.cBIGFI-transmits sensitive or security-om/supp011117/critical data in cleartext in aort/docvi31communication channel that canew.wss?uibe sniffed by unauthorized actors.d=swg22IBM X-Force ID: 123911.009673 CVE ID : CVE-2017-1232
Gain Information	26-10-2017	4.3	IBM Tivoli Endpoint Manager (IBMhttp://wA-IBM-BigFix Platform 9.2 and 9.5) couldww.ibm.cBIGFI-allow a remote attacker to obtainom/supp011117/sensitive information, caused byort/docvi32the failure to properly enable theew.wss?uisecurecookieattribute.Andd=swg22attackercouldexploitthis009673ulnerability to obtain sensitiveinformationusingmiddletechniques.IBM X-Forceuncenter
CV Scoring Scale (C	VSS)	0-1	1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10
Vulnerability Type	(s): quest Forgery; Dir	. TravDir	rectory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ID: 123907.		
Gain Information	26-10-2017	5	CVE ID : CVE-2017-1228 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://w ww.ibm.c om/supp ort/docvi ew.wss?ui d=swg22 009673	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://w ww.ibm.c om/supp ort/docvi ew.wss?ui d=swg22 009673	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://w ww.ibm.c om/supp ort/docvi ew.wss?ui d=swg22 009673	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://w ww.ibm.c om/supp ort/docvi ew.wss?ui d=swg22 009673	A-IBM- BIGFI- 011117/ 36
Daeja Viewone					ſ
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://w ww.ibm.c om/supp ort/docvi ew.wss?ui d=swg22	A-IBM- DAEJA- 011117/ 37
CV Scoring Scale (C	VSS)	0-1	1-2 2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10
Vulnerability Type	(s): quest Forgery; Dir	. TravDir	ectory Traversal; DoS-Denial of Service; NA- N	ot Applicable; S	ql-SQL

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID Patch NCIIPC II				
	Date		CVE ID : CVE-2017-1211 008011				
XSS	24-10-2017	3.5	IBM Daeja ViewONE Professional, Standard & Virtual 4.1.5.1 and ww.ibm.cA-IBM- DAEJA- 0AEJA- 011117/ scripting. This vulnerability allows 				
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.http://w ww.ibm.c om/suppA-IBM- DAEJA- 011117/ 39CVE ID : CVE-2017-1212d=swg22 007466				
NA	24-10-2017	5	IBM Daeja ViewONE Professional, Standard & Virtual 4.1.5.1 and allow an om/supp 011117/ unauthenticated attacker to inject data into log files made to look legitimate. IBM X-Force ID: 123850. CVE ID : CVE-2017-1210http://w <br< td=""></br<>				
Irfanview			· · · · · ·				
Babacad4imag	je;Irfanview						
DoS Overflow	22-10-2017	6.8	IrfanView4.50-64bitwithhttps://giA-IRF-BabaCAD4Imagepluginversionthub.comBABAC-1.3allowsattackers to cause a/wlinzi/s011117/denial ofservice or possibly haveecurity_a41unspecifiedotherimpactviadvisoriescrafted.dwg file, related to"Data/tree/mafromFaultingAddresscontrolsster/CVE-BranchSelectionstartingat2017-BabaCAD4Image!ShowPlugInOptio15766ister/CVE-ns+0x0000000001f0a0."useuseuseCVE ID:CVE-2017-15766useuse				
DoS Overflow	22-10-2017	6.8	IrfanView4.50-64bitwithhttps://giA-IRF-BabaCAD4Imagepluginversionthub.comBABAC-1.3allowsattackerstocausea/wlinzi/s011117/denialofserviceorunspecifiedotherimpactviadvisories42crafted.dwgfile, relatedtoa/tree/ma				
CV Scoring Scale (C	VSS)	0-1	1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-1				
CSRF-Cross Site Rec	CV Scoring Scale (CVSS) Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. TravDirectory 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 Violation starting at BabaCAD4Image!ShowPlugInOptio ns+0x00000000001e6b0." 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!ShowPlugInOptio ns+0x0000000001eca0." CVE ID : CVE-2017-15763	https://gi thub.com /wlinzi/s ecurity_a dvisories /tree/ma ster/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!ShowPlugInOptio ns+0x0000000001f31b." CVE ID : CVE-2017-15762	https://gi thub.com /wlinzi/s ecurity_a dvisories /tree/ma ster/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!ShowPlugInOptio ns+0x0000000001ecaa." CVE ID : CVE-2017-15761	https://gi thub.com /wlinzi/s ecurity_a dvisories /tree/ma ster/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!ShowPlugInOptio ns+0x0000000001ce82." CVE ID : CVE-2017-15760	https://gi thub.com /wlinzi/s ecurity_a dvisories /tree/ma ster/CVE- 2017- 15760	A-IRF- BABAC- 011117/ 46	
DoS Execute	22-10-2017	6.8	IrfanView 4.50 - 64bit with	https://gi	A-IRF-	
DOS Execute 22-10-2017 0.8 Intaliview 4.50 - 04 bit Intips://gi A-IKF- 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)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Code	Date		BabaCAD4Image plugin version	thub.com	BABAC-
Overflow			1.3 allows attackers to Execute	/wlinzi/s	011117/
			arbitrary code or cause a denial of	ecurity_a	47
			service via a crafted .dwg file,	dvisories	
			related to a "User Mode Write AV	/tree/ma	
			near NULL starting at	ster/CVE-	
			BabaCAD4Image!ShowPlugInOptio	2017-	
			ns+0x000000000001b3f3."	15759	
			CVE ID : CVE-2017-15759		
DoS Execute	22-10-2017	6.8	IrfanView 4.50 - 64bit with	https://gi	A-IRF-
Code			BabaCAD4Image plugin version	thub.com	BABAC-
Overflow			1.3 allows attackers to Execute	/wlinzi/s	011117/
			arbitrary code or cause a denial of	ecurity_a	48
			service via a crafted .dwg file,	dvisories	
			related to "Data from Faulting	/tree/ma	
			Address controls subsequent	ster/CVE-	
			Write Address starting at	2017-	
			BabaCAD4Image!ShowPlugInOptio	15758	
			ns+0x000000000004d75b."		
			CVE ID : CVE-2017-15758		
DoS Overflow	22-10-2017	6.8	IrfanView 4.50 - 64bit with	https://gi	A-IRF-
			BabaCAD4Image plugin version	thub.com	BABAC-
			1.3 allows attackers to cause a	/wlinzi/s	011117/
			denial of service or possibly have	ecurity_a	49
			unspecified other impact via a	dvisories	
			crafted .dwg file, related to "Data	/tree/ma	
			from Faulting Address controls	ster/CVE-	
			Branch Selection starting at	2017-	
			BabaCAD4Image!ShowPlugInOptio	15757	
			ns+0x00000000000029ba."		
	22 10 2017	6.0	CVE ID : CVE-2017-15757		
DoS Execute	22-10-2017	6.8	IrfanView 4.50 - 64bit with	https://gi	A-IRF-
Code			BabaCAD4Image plugin version	thub.com	BABAC-
Overflow			1.3 allows attackers to Execute	/wlinzi/s	011117/
			arbitrary code or cause a denial of	ecurity_a	50
			service via a crafted .dwg file,	dvisories	
			related to "Data from Faulting	/tree/ma	
			Address controls subsequent	ster/CVE-	
			Write Address starting at	2017- 15756	
			BabaCAD4Image!ShowPlugInOptio ns+0x00000000004d7c4."	15/50	
			CVE ID : CVE-2017-15756		
DoS Overflow	22-10-2017	6.8	IrfanView 4.50 - 64bit with	https://gi	A-IRF-
	22 10-201/	0.0	BabaCAD4Image plugin version	thub.com	BABAC-
			1.3 allows attackers to cause a	/wlinzi/s	011117/
			denial of service or possibly have	ecurity_a	51
		0-1		6-7 7-8	8-9 9-1
CV Scoring Scale (CV	(221)	0-1			

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!AVrfpDphFindBusyMemor yNoCheck+0x000000000000091 ." CVE ID : CVE-2017-15755	dvisories /tree/ma ster/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!ShowPlugInOptio ns+0x00000000013968." CVE ID : CVE-2017-15754	https://gi thub.com /wlinzi/s ecurity_a dvisories /tree/ma ster/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!ShowPlugInOptio ns+0x000000000029c2." CVE ID : CVE-2017-15753	https://gi thub.com /wlinzi/s ecurity_a dvisories /tree/ma ster/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!ShowPlugInOptio ns+0x0000000004d6b0." CVE ID : CVE-2017-15752	https://gi thub.com /wlinzi/s ecurity_a dvisories /tree/ma ster/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://gi thub.com /wlinzi/s ecurity_a dvisories /tree/ma ster/CVE-	A-IRF- BABAC- 011117/ 55
CV Scoring Scale (CV	/SS)	0-1	1-2 2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Vulnerability Type(s)	Publish Date	CVSS	Desc	ription & CV	E ID	Pate	ch	NCIIPC	ID
			ns+0x0000 CVE ID : CV	mage!ShowP 000000009f3 E-2017-157	9." 51	2017- 15751			
DoS Overflow	22-10-2017	6.8	1.3 allows denial of se unspecified crafted .dw Access V BabaCAD4I ns+0x0000	mage plugin attackers to ervice or pos other imp g file, related	n version o cause a sibly have act via a to a "Read urting at lugInOptic e0."	thub.c /wlinz ecurit dvisor /tree/ ster/C	zi/s y_a ries (ma CVE-	A-IRF- BABAC 011117 56	
Cadimage;Irfa	1		r						
DoS Execute Code Overflow	22-10-2017	6.8	CADImage allows at arbitrary co service via related to a near N CADIMAGE	4.50 - 64 plugin version tackers to ode or cause a crafted "User Mode ULL start +0x00000000 CVE-2017-1	n 12.0.0.5 Execute a denial of .dwg file Write AV ting at 0003d5b5	thub.c /wlinz ecurit dvisor /tree/	zi/s y_a ries (ma CVE-	A-IRF- CADIM- 011117 57	
DoS Overflow	22-10-2017	6.8	allows atta of service unspecified crafted .dw from Faulti one or m subsequent at CADIMAGE	4.50 - 64 plugin versio ckers to caus or possi other imp g file, related ng Address ore argume Function Ca +0x000000000 CVE-2017-1	n 12.0.0.5 e a denial bly have act via a d to "Data is used as ents in a all starting 0003e946	thub.c /wlinz ecurit dvisor /tree/ ster/C 2017-	zi/s y_a ries 'ma ZVE-	A-IRF- CADIM 011117 58	
DoS Overflow	22-10-2017	6.8	allows atta of service unspecified crafted .dw from Fault Branch S CADIMAGE	plugin versio ckers to caus or possi other imp g file, related ing Address	n 12.0.0.5 e a denial bly have act via a d to "Data controls arting at 0000348b	thub.c /wlinz ecurit dvisor /tree/ ster/C	zi/s y_a ries 'ma ZVE-	A-IRF- CADIM- 011117 59	
DoS Execute	22-10-2017	6.8	IrfanView		lbit with	https:/	//gi	A-IRF-	
CV Scoring Scale (C	VSS)	0-1	1-2 2-3	3-4 4-5	5-6		7-8	8-9	9-10
Vulnerability Type CSRF-Cross Site Rec Injection; XSS- Cros	quest Forgery; Dir	. TravDii	rectory Traversa	l; DoS-Denial of	Service; NA-	Not Applic	able; Sc	ll-SQL	

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Code	Date		CADImage plugin version 12.0.0.5	thub.com	CADIM-
Overflow			allows attackers to Execute	/wlinzi/s	011117/
			arbitrary code or cause a denial of service via a crafted .dwg file,	ecurity_a dvisories	60
			related to a "User Mode Write AV	/tree/ma	
			starting	ster/CVE-	
			CADIMAGE+0x0000000000000613	2017-	
			a." CVE ID : CVE-2017-15748	15748	
DoS Execute	22-10-2017	6.8	IrfanView 4.50 - 64bit with	https://gi	A-IRF-
Code			CADImage plugin version 12.0.0.5	thub.com	CADIM-
Overflow			allows attackers to Execute	/wlinzi/s	011117/
			arbitrary code or cause a denial of	ecurity_a	61
			service via a crafted .dwg file,	dvisories	
			related to a "Data Executeution	/tree/ma	
			Prevention Violation starting at	ster/CVE-	
			Unknown Symbol @ 0x0000700b00260112 called from	2017- 15747	
			CADIMAGE+0x00000000003d35a	15/4/	
			d." CVE ID : CVE-2017-15747		
DoS Overflow	22-10-2017	6.8	IrfanView 4.50 - 64bit with	https://gi	A-IRF-
		0.0	CADImage plugin version 12.0.0.5	thub.com	CADIM-
			allows attackers to cause a denial	/wlinzi/s	011117/
			of service or possibly have	ecurity_a	62
			unspecified other impact via a	dvisories	
			crafted .dwg file, related to "Data	/tree/ma	
			from Faulting Address controls	ster/CVE-	
			Branch Selection starting at	2017-	
			CADIMAGE+0x0000000003d21b	15746	
			3." CVE ID : CVE-2017-15746		4 15 5
DoS Overflow	22-10-2017	6.8	IrfanView 4.50 - 64bit with	https://gi	A-IRF-
			CADImage plugin version 12.0.0.5 allows attackers to cause a denial	thub.com	CADIM-
			of service or possibly have	/wlinzi/s ecurity_a	011117/ 63
			unspecified other impact via a	dvisories	03
			crafted .dwg file, related to "Data	/tree/ma	
			from Faulting Address controls	ster/CVE-	
			Branch Selection starting at	2017-	
			CADIMAGE+0x000000000002ca2	15745	
			e." CVE ID : CVE-2017-15745		
DoS Execute	22-10-2017	6.8	IrfanView 4.50 - 64bit with	https://gi	A-IRF-
Code			CADImage plugin version 12.0.0.5	thub.com	CADIM-
Overflow			allows attackers to Execute	/wlinzi/s	011117/
			arbitrary code or cause a denial of	ecurity_a	64
			service via a crafted .dwg file,	dvisories	
			related to a "Read Access Violation	/tree/ma	
	 	0-1	onControlFlowstartingat1-22-33-44-55-60	ster/CVE-	8-9 9-10
CV Scoring Scale (CV		· ·			

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Type(s)	Date		CADIMAGE+0x00000000003d35a	2017-	
			7." CVE ID : CVE-2017-15744	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+0x000000003d24a 0." CVE ID : CVE-2017-15743	https://gi thub.com /wlinzi/s ecurity_a dvisories /tree/ma ster/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+0x000000003d232 8." CVE ID : CVE-2017-15742	https://gi thub.com /wlinzi/s ecurity_a dvisories /tree/ma ster/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+0x0000000003d237 8." CVE ID : CVE-2017-15741	https://gi thub.com /wlinzi/s ecurity_a dvisories /tree/ma ster/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+0x0000000033228 e." CVE ID : CVE-2017-15740	https://gi thub.com /wlinzi/s ecurity_a dvisories /tree/ma ster/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://gi thub.com /wlinzi/s ecurity_a dvisories	A-IRF- CADIM- 011117/ 69
		0-1	1-2 2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Vulnerability Type(s)	Publish Date	CVSS	Desc	cription & CVE	ID]	Patch	NCIIPC	ID
			Address Write A CADIMAGE	"Data from controls su ddress star +0x00000000 : CVE-2017-15	bsequent ting at 000042d	ste 20	ree/ma er/CVE- 17- 739		
DoS Overflow	22-10-2017	6.8	allows atta of service unspecified crafted .dw Access V CADIMAGE	4.50 - 64 plugin version ockers to cause e or possib d other impa g file, related t violation stan c+0x00000000 cVE-2017-15	a 12.0.0.5 a denia ly have ct via a o a "Read ting at 003d22d	thu /w ecu dv /tr ste 20	ps://gi ub.com dinzi/s urity_a isories ree/ma er/CVE- 17- 738	A-IRF- CADIM- 011117 70	
DoS Overflow	22-10-2017	6.8	IrfanView CADImage allows atta of service unspecified crafted .dw Access V CADIMAGE	4.50 - 64 plugin version ickers to cause e or possib d other impa rg file, related t	oit with 12.0.0.5 a denia ly have ct via a o a "Read ting at 003d246	htt htt w ecu dv /tr ste 20	ps://gi ub.com dinzi/s urity_a isories ree/ma er/CVE- 17- 737	A-IRF- CADIM- 011117 71	
Irfanview DoS Execute Code Overflow	22-10-2017	6.8	allows a arbitrary c service via mishandled render the "Data fro controls Address ntdll!memo	version 4.50 ttackers to ode or cause a a crafted .dll f d during an at e DLL icon, r om Faulting subsequent starting cpy+0x000000 D : CVE-2017-	Execute denial of ile that is tempt to elated to Address Write at 0000000	thu f /w ecu dv /tr ste 20	ps://gi ub.com dinzi/s urity_a isories ree/ma er/CVE- 17- 800	A-IRF- IRFAN- 011117 72	
DoS Overflow	22-10-2017	6.8	IrfanView allows atta of service unspecified crafted .dll during an DLL icon, Faulting A Selection KERNELBA	version 4.50 ockers to cause	(64bit) a denia ly have ct via a shandled nder the ata from s Branch at	thu e /w ecu dv: /tr ste 20 : 15	ps://gi ub.com dinzi/s urity_a isories ree/ma er/CVE- 17- 799	A-IRF- IRFAN- 011117 73	
		0-1	1-2 2-3	3-4 4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	CVSS		Desc	riptior	a & CVE	ID		Patch	NCIIPC	ID
Type(3)	Dutt		." C\	/E ID : (CVE-20	17-157	799				
DoS Overflow	22-10-2017	6.8	Irfan allov of unsj craff duri DLL Faul Sele KER esIn ." CV	nView ws atta service pecified ted .dll ing an icon, iting Ac ction NELBA ternal+ 'E ID : C	versio ckers t e or l other file tha attemp related ddress s SE!Enu 0x0000 CVE-20	n 4.50 o cause possib r impa at is mi ot to re l to "D control tarting mReso 000000 17-157) (64b e a den oly ha ct via ishandl ender t ata fro s Bran urceNa 000060	ial th ve / ed d he / om st om st at 1 m 09	ttps://gi nub.com wlinzi/s curity_a visories tree/ma ter/CVE- 017- 5798	A-IRF- IRFAN- 011117 74	/
DoS Execute Code Overflow	22-10-2017	6.8	allov arbi serv misl renc "Rea Data TOC 000	trary co vice via handlec ler the ad Acco	tackers ode or a crafte l durin DLL io ess Vio love oadIma 0b9."	s to cause a ed .dll f g an at con, rel lation starti ge_W+(Exect denial ile that ttempt ated to on Blo ng 0x0000	te th of / is e to d o a / ock st at 2	ttps://gi nub.com wlinzi/s curity_a visories tree/ma ter/CVE- 017- 5797	A-IRF- IRFAN- 011117 75	/
DoS Overflow	22-10-2017	6.8	Irfan allov of unsj crafi duri DLL Viol ntdl U+0	nView ws atta	versio ckers t e or l other file that attemp elated t s earchR 000000	n 4.50 o cause possib r impa at is mi ot to re o a "Rea tarting esource 000386	(64b e a den ly ha ct via ishandl ender t ad Acce eSectio	ial th ive / a e ed d the / ess st at 2	ttps://gi nub.com wlinzi/s curity_a visories tree/ma ter/CVE- 017- 5796	A-IRF- IRFAN- 011117 76	/
DoS Overflow	22-10-2017	6.8	Irfan allov of unsj craf duri DLL Viol ntdl U+0	nView ws atta service pecified ted .dll ing an icon, ro ation l!LdrpS x00000	versio ckers t e or l other file that attemp elated t s earchR 000000	n 4.50 o cause possib impa at is mi ot to re o a "Rea tarting esource 0002bc	(64b e a den ly ha ct via ishandl ender t ad Acce eSectio	ial th ve / ed d he / ess st at II n_ 2	ttps://gi nub.com wlinzi/s curity_a visories tree/ma ter/CVE D :CVE- 017- 5795	A-IRF- IRFAN- 011117 77	/
CV Scoring Scale (C	VSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
CV Scoring Scale (C Vulnerability Type CSRF-Cross Site Rec Injection; XSS- Cros	(s): quest Forgery; Dir										

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!LdrpResSearchResourceInsid eDirectory+0x0000000000025 7." CVE ID : CVE-2017-15794	https://gi thub.com /wlinzi/s ecurity_a dvisories /tree/ma ster/CVE- 2017- 15794	A-IRF- IRFAN- 011117/ 78
DoS Execute Code Overflow	22-10-2017	6.8	7. CVEID: CVE-2017-13794IrfanView version 4.50 (64bit)allows attackers to Executearbitrary code or cause a denial ofservice via a crafted .dll file that ismishandled during an attempt torender the DLL icon, related to"Data from Faulting AddresscontrolssubsequentAddressstartingatntdll!memcpy+0x00000000000000000000000000000000000	https://gi thub.com /wlinzi/s ecurity_a dvisories /tree/ma ster/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!EnumResourceType sInternal+0x0000000000007b2." CVE ID : CVE-2017-15792	https://gi thub.com /wlinzi/s ecurity_a dvisories /tree/ma ster/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!LdrpResCompareResourceNa mes+0x000000000000000." CVE ID : CVE-2017-15791	https://gi thub.com /wlinzi/s ecurity_a dvisories /tree/ma ster/CVE- 2017- 15791	A-IRF- IRFAN- 011117/ 81

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
DoS Overflow	22-10-2017	6.8	IrfanView version 4.50 (64bit)	https://gi	A-IRF-
			allows attackers to cause a denial	thub.com	IRFAN-
			of service or possibly have	/wlinzi/s	011117/
			unspecified other impact via a	ecurity_a	82
			crafted .dll file that is mishandled	dvisories	
			during an attempt to render the DLL icon, related to a "Read Access	/tree/ma ster/CVE-	
			Violation starting at	2017-	
			ntdll!LdrpResCompareResourceNa	15790	
			mes+0x00000000000000120."	10770	
			CVE ID : CVE-2017-15790		
DoS Overflow	22-10-2017	6.8	IrfanView 4.50 - 64bit allows	https://gi	A-IRF-
			attackers to cause a denial of	thub.com	IRFAN-
			service or possibly have	/wlinzi/s	011117/
			unspecified other impact via a	ecurity_a	83
			crafted .dds file, related to "Read	dvisories	
			Access Violation starting at	/tree/ma	
			FORMATS!ReadBLP_W+0x000000	ster/CVE-	
			0000001b22."	2017- 15769	
DoS Overflow	22-10-2017	6.8	CVE ID : CVE-2017-15769 IrfanView version 4.50 - 64bit	https://gi	A-IRF-
D03 Over now	22-10-2017	0.0	allows attackers to cause a denial	thub.com	IRFAN-
			of service or possibly have	/wlinzi/s	011117/
			unspecified other impact via a	ecurity_a	84
			crafted .tif file, related to "Data	dvisories	
			from Faulting Address controls	/tree/ma	
			Branch Selection starting at	ster/CVE-	
			image000007f7_42060000+0x000	2017-	
			000000094113."	15768	
<u> </u>			CVE ID : CVE-2017-15768		
Irssi Irssi					
NA	22-10-2017	5	In Irssi before 1.0.5, overlong nicks	https://ir	A-IRS-
			or targets may result in a NULL	ssi.org/se	IRSSI-
			pointer dereference while splitting	curity/irs	011117/
			the message.	si_sa_201	85
			CVE ID : CVE-2017-15723	7_10.txt	
NA	22-10-2017	5	In certain cases, Irssi before 1.0.5	https://ir	A-IRS-
			may fail to verify that a Safe	ssi.org/se	IRSSI-
			channel ID is long enough, causing	curity/irs	011117/8
			reads beyond the end of the string. CVE ID : CVE-2017-15722	si_sa_201	6
NA	22-10-2017	5	In Irssi before 1.0.5, certain	7_10.txt http://op	A-IRS-
1141	22 10 2017	3	incorrectly formatted DCC CTCP	enwall.co	IRSSI-
			messages could cause a NULL	m/lists/o	011117/
1			pointer dereference. This is a	SS-	87
			pointer dereierence. This is a	33	07

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://ir ssi.org/se curity/irs si_sa_201 7_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://ir ssi.org/se curity/irs si_sa_201 7_10.txt	A-IRS- IRSSI- 011117/ 89
Labwiki Projec	ct				
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	1				
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	10.10.0015	4		hu //	
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://p habricato r.wikimed ia.org/T4 1823	A-MED- MEDIA- 011117/ 92
NA	19-10-2017	4.3	MediaWiki before 1.18.5, and	https://p	A-MED-
CV Scoring Scale (C	VSS)	0-1	1-2 2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10
Vulnerability Type	_				
		. TravDir	ectory Traversal; DoS-Denial of Service; NA- N	ot Applicable; S	ql-SQL

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	habricato r.wikimed ia.org/T4 1180	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://p habricato r.wikimed ia.org/T3 9587	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://b ugzilla.re dhat.com /show_bu g.cgi?id=8 53409	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://p habricato r.wikimed ia.org/T4 1824	A-MED- MEDIA- 011117/ 96
Octopus			CVL ID . CVL 2012 4300		
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://gi thub.com /Octopus Deploy/Is sues/issu es/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://gi thub.com /Octopus Deploy/Is sues/issu	A-OCT- OCTOP- 011117/ 98
CV Scoring Scale (C	VSS)	0-1	1-2 2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10
Vulnerability Type CSRF-Cross Site Rec		. TravDir	ectory Traversal; DoS-Denial of Service; NA- N	ot Applicable; S	ql-SQL

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.es/3869CVE ID : CVE-2017-15610
Gain Information	19-10-2017	5	Octopusbefore3.17.7allowshttps://giA-OCT-attackerstoobtainsensitivethub.comOCTOP-cleartextinformationby reading a/Octopus011117/variableJSONfileincertainDeploy/IssituationsinvolvingOfflineDropsues/issuTargets.es/3868es/3868
Oracle			
Access Manage			
Gain Information	19-10-2017	5	Vulnerability in the Oracle Accesshttp://wA-ORA-Manager component of Oracleww.oraclACCES-FusionMiddlewaree.com/tec011117/(subcomponent:WebServerhnetwork100Plugin).The supported version/security-that is affected is 11.1.2.3.0.Easilyadvisory/exploitablevulnerabilityallowscpuoct20unauthenticatedattackerwithnetworkaccessviaManager.Successful attacks of thishtmlwulnerabilitycanresultinunauthorizedreadaccesshtmlunauthorizedreadaccesshtmlunauthorizedreadaccesshtmlwulnerabilitycanresultinunauthorizedreadaccesshtmlunauthorizedreadaccesshtmlunauthorizedreadaccesshtmlwulnerabilitycanresultinunauthorizedreadaccesshtmlunauthorizedreadaccesshtmlunauthorizedcVSSVector:in(CVSS:3.0/AV:N/AC:L/PR:N/UI:N/ininS:U/C:L/I:N/A:N).ininCVE ID:CVE-2017-10154in
Advanced Outb	ound Telepho	ony	
NA	19-10-2017	5.8	VulnerabilityintheOraclehttp://wA-ORA-AdvancedOutboundTelephonyww.oraclADVAN-componentofOracleE-Businesse.com/tec011117/Suite(subcomponent:Setupandhnetwork101Configuration).Supported/security-versionsthatareaffectedareadvisory/12.2.3,12.2.4,12.2.5,12.2.6andcpuoct2012.2.7.Easilyexploitable17-vulnerabilityallows3236626.
CV Scoring Scale (C	VSS)	0-1	1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10
Vulnerability Type	(s): quest Forgery; Dir	. TravDii	rectory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL

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).	html	
NA	19-10-2017	5.8	CVE ID : CVE-2017-10417VulnerabilityintheOracleAdvancedOutboundTelephonycomponentofOracleE-BusinessSuite(subcomponent:SetupandConfiguration).Supportedversionsthatareaffectedversionsthatareaffectedare12.2.3,12.2.4,12.2.5,12.2.6and12.2.7.EasilyexploitablevulnerabilityallowsunauthenticatedattackerwithnetworkaccessviaHTTPtocompromiseOracleAdvancedOutboundTelephony.SuccessfulattacksrequirehumaninteractionfromapersonotherthanattackerandwhilethevulnerabilityisinOracleAdvancedOutboundTelephony,attacksmaysignificantlyimpactadditionalproducts.Successful attacks of thisvulnerabilitycan	hnetwork	A-ORA- ADVAN- 011117/ 102
CV Scoring Scale (C	VSS)	0-1	1-2 2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10
Vulnerability Type CSRF-Cross Site Rec Injection; XSS- Cros	quest Forgery; Dir	. TravDir	ectory Traversal; DoS-Denial of Service; NA- N	lot Applicable; S	iql-SQL

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
- 5 F - (- 5			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 Engineer		agemen			
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://w ww.oracl e.com/tec hnetwork /security- advisory/ cpuoct20 17- 3236626. html	A-ORA- AGILE- 011117/ 103
Agile Product I	Lifecycle Mana	igement		I	
NA	19-10-2017	3.6	Vulnerability in the Oracle AgilePLM component of Oracle SupplyChainProductsSubcomponent:Performance).Supportedversionsthatare	http://w ww.oracl e.com/tec hnetwork /security-	A-ORA- AGILE- 011117/ 104
CV Scoring Scale (C	VSS)	0-1	1-2 2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10
Vulnerability Type	(s): quest Forgery; Dir	: TravDir	rectory Traversal; DoS-Denial of Service; NA- N	ot Applicable; S	ql-SQL

Vulnerability	Publish	CVSS	Description & CVE IDPatchNCIIPC ID
Type(s) Gain Information	Date	4	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
			affected are 9.3.5 and 9.3.6. Easily exploitable vulnerability allows privileged attacker with network access via HTTP to 3236626.counce 3236626.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).advisory/ cpuoct20 17- 3236626.CVE ID : CVE-2017-10299advisory
Application Ob			
Gain Information	19-10-2017	5	VulnerabilityintheOraclehttp://wA-ORA-ApplicationObjectLibraryww.oraclAPPLI-componentofOracleE-Businesse.com/tec011117/Suite(subcomponent:hnetwork106Diagnostics).Supported versions/security-that are affected are 12.1.3, 12.2.3,advisory/12.2.4, 12.2.5, 12.2.6 and 12.2.7.Easilyexploitablevulnerability17-allowsunauthenticatedattacker3236626.
CV Scoring Scale (CV	VSS)	0-1	1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10
Vulnerability Type(CSRF-Cross Site Req Injection; XSS- Cros	quest Forgery; Dir	. TravDir	rectory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL

Vulnerability	Publish	CVSS	Description & CVE IDPatchNCIIPC ID
Type(s) Gain Information	Date	5	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
Applications D	1		
NA	19-10-2017	5.5	VulnerabilityintheOraclehttp://wA-ORA-ApplicationsDBAcomponentofww.oraclAPPLI-OracleE-BusinessSuitee.com/tec011117/(subcomponent:ADUtilities).hnetwork108Supportedversionsthatare/security-affected are12.1.3,12.2.3,12.2.4,advisory/12.2.5,12.2.6and12.2.7.Easilycpuoct20exploitablevulnerabilityallows17-highprivilegedattackerwith3236626.networkaccessviaHTTPtohtmlcompromiseOracleApplications
CV Scoring Scale (CV	VSS)	0-1	1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10
Vulnerability Type(CSRF-Cross Site Req Injection; XSS- Cros	uest Forgery; Dir	. TravDii	rectory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL

Vulnerability Type(s)	Publish Date	CVSS	De	scription	& CVE	ID		Patch	NCI	PC ID
			DBA. Su vulnerab unauthor modificat or all C accessibl unauthor data or Oracle accessibl Score 6 Integrity (CVSS:3.0 S:U/C:H/ CVE ID :	ility ca ized crea ion acces oracle Ap e data ized acc complete Applic e data. .5 (Conf impacts)/AV:N/A I:H/A:N).	n re tion, de s to cri oplicatio as cess to e acces ations CVSS fidentia). CVSS C:L/PR	sult eletion tical da ons DE well critic ss to a DE 3.0 Bas lity ar S Vecto :H/UI:N	in or ta BA as cal all BA se nd or:			
Business Intell	V	1								
NA	19-10-2017	4.9	Vulnerab Business Edition Fusion (subcomj General). are aff 11.1.1.9.0 12.2.1.2.0 vulnerab attacker HTTP t Business Edition. S human in other tha attacks of result in deletion critical d Intelligen accessibl unauthor subset Intelligen accessibl to href="htt CSP/main e=NOT&i	Intellige component: Supporte fected a b, 12 b, Easi ility allow with net o comp Intellige Successful nteraction n the atta of this v unauthor or modifi ata or all nee Ente e data ized rea of Or nee Ente e data. No Doc p://supp n/article?	ence E ent of Mi Analyt: ed vers are 1 .2.1.1.0 ly ex vs low p work a promise ence E l attack n from acker. S ulnerat orized cation Oracle erprise as d acce acle erprise to acce as cacle erprise ort.orac	f Orac ddlewa ics We ions th 1.1.1.7. ar cploitab privilege ccess v orac nterpri s requi a perso bility ca creatio access Busine Editio ess to Busine Editio case ref cle.com, now&ty	se ww le e.c. re hr. eb /s at ad .0, cp nd 17 le 32 ed ht le se re on ful an, to ss on as as on er <a /p</a 	tp://w w.oracl com/tec etwork ecurity- visory/ uoct20 '- 236626. ml	A-OI BUS 0111 109	
CV Scoring Scale (C	VSS)	0-1	1-2 2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type CSRF-Cross Site Rec Injection; XSS- Cros	uest Forgery; Dir	. TravDii	rectory Trave	rsal; DoS-D	enial of S	ervice; NA	A- Not A	pplicable; S	Sql-SQL	

Vulnerability Type(s)	Publish Date	CVSS		Descr	iptio	n & CV	E ID		Р	atch	NC	IIPC ID
			instructure this i (Continue impa (CVS) S:U/(ssue. C fidentia cts).	on VSS 3. llity CV V:N/A /A:N).	.0 Base and /SS AC:L/PI	o addr e Score Integ Vect R:L/UI:	6.3 rity tor:				
NA	19-10-2017	5.8	Vulne Busin Editio Fusic (subo Gene are 11.1. 12.2. vulne unau netw comp Intell Succe inter than vulne Intell attac addit attac resul critic all (Enter Succe inser Oracl Enter CVSS (Cont impa (CVS) S:C/O	erability ness Ir on co on compone ral). Su affect 1.9.0, 1.2.0. erability thentice ork ac oromise igence essful a action the at erability igence ks may ional ks of t in un al data Oracle cprise H rell as t or de for to for t or de for to for t as t or de for to for t or to for t or to for t or to for t or de for to for t or to for to for to for t or to for to for t or to for to for to for t or to for to for to for to for t or to for to for to for to for to for to for to for t or to for to fo	y ir ntellig mpon ent: pport ed 12 Easi / ated ccess from tacker / sigr produ tacker / sigr produ tacker / sigr produ this v nautho or co Busin Edition unaut lete a usines Editior Bas lity V:N/A /A:N).	n the ence ent o M Analy ced ver are 2.2.1.1.1 ily e attack via racle erprise s requi a per r and Oracle erprise s requi a per r and Oracle erprise s requi a per r and oracle erprise s requi a per r and oracle enficant ucts. vulnera orized omplete s s lin n access thorize ccess t s and VSS AC:L/PI	e Ora Enterpro of Ora liddlew tics V rsions t 11.1.1. 0 a exploita allo ker w HTTP Busin e Editi tire hun son ot while e Editi tire hun son ot soluti soluti to some sible d core Integ Vect R:N/UI:	acle vare Veb chat 7.0, and ble ows vith to ness ion. her the ness ion. her the ess ion. her the sto nce lata ate, e of nce ata. 8.2 rity tor:	ww e.cc hne /se adv cpu 17-	86626.	BU 01 11	DRA- SIN- 1117/ D
Business Intell	Ŭ		L							_		
Gain	19-10-2017	5		erabilit		_	Oracle	BI		o://w		DRA-
CV Scoring Scale (C	-	0-1	1-2	2-3	3-4	4-5	5-6	e	6-7	7-8	8-9	9-10
Vulnerability Type CSRF-Cross Site Rec Injection; XSS- Cros	quest Forgery; Dir	. TravDii	ectory]	[raversal	; DoS-D	enial of	Service;	NA- No	ot Apj	plicable;	Sql-SQ	L

Vulnerability	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Type(s) 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).	ww.oracl e.com/tec hnetwork /security- advisory/ cpuoct20 17- 3236626. html	BUSIN- 011117/ 111
NA	19-10-2017	5.8	CVE ID : CVE-2017-10037Vulnerability in the Oracle BIPublisher component of OracleFusionMiddleware(subcomponent: Core FormattingAPI). Supported versions that areaffected are 11.1.1.7.0 and11.1.1.9.0.Easily exploitablevulnerabilityallowsunauthenticated attacker withnetwork access via HTTP tocompromise Oracle BI Publisher.Successful attacks require humaninteraction from a person otherthan the attacker and while thevulnerability is in Oracle BIPublisher, attacks maysignificantly impact additionalproducts. Successful attacks of thisvulnerability can result inunauthorized access to allOracle BI Publisher accessible dataas well as unauthorized update,insert or delete access to some ofOracle BI Publisher accessible	http://w ww.oracl e.com/tec hnetwork /security- advisory/ cpuoct20 17- 3236626. html	A-ORA- BUSIN- 011117/ 112

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
<u> </u>	Date		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 Appli	cations				
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://w ww.oracl e.com/tec hnetwork /security- advisory/ cpuoct20 17- 3236626. html	A-ORA- COMMO- 011117/ 113
Common Appli	cations Calen	dar	CVE ID : CVE-2017-10330		
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://w ww.oracl e.com/tec hnetwork /security- advisory/ cpuoct20 17- 3236626. html	A-ORA- COMMO- 011117/ 114
CV Scoring Scale (C	VSS)	0-1	1-2 2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10
Vulnerability Type CSRF-Cross Site Rec Injection; XSS- Cros	luest Forgery; Dir	. TravDii	rectory Traversal; DoS-Denial of Service; NA- N	ot Applicable; S	ql-SQL

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID Patch NCIIPO	D
	10 10 2017		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). 	
NA	19-10-2017	5.8	VulnerabilityintheOraclehttp://wA-ORACommonApplicationsCalendarww.oraclCOMMcomponentof OracleE-Businesse.com/tec011112ApplicationsCalendar).Supported/security-versionsthatareaffectedadvisory/12.1.1,12.1.2,12.1.3,12.2.3,cpuoct2012.2.4,12.2.5,12.2.6and12.2.7.17-Easilyexploitablevulnerability3236626.htmlallowsunauthenticatedattackerhtmlitmlwithnetworkaccess viaHTTP tocompromisecompromiseOracleCommonApplicationsCalendar.ApplicationsCalendar.Successfulattacksritmlattackerandwhilethevulnerability is inoracleoraclecommonApplicationsCalendar, attacks maysignificantlyimpactadditionalproducts.Successfulattacks of thisvulnerabilitycanresultvulnerabilitycanresultinunauthorizedaccess to alloraclecommonApplicationsCalendaraccess to alloraclecommonApplicationscalendaraccessibledata.CVSS3.0Basescore8.2(ConfidentialityandIntegrityimpacts).CVSSVector:(CVSS:3.0/AV:N/AC:L/PR:N/UI:R/sc/C:H/I:L/A	0-
NA	19-10-2017	5.8	Vulnerability in the Oracle http://w A-ORA	
CV Scoring Scale (C		0-1	1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9	9-10
Vulnerability Type				

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.oracl e.com/tec hnetwork /security- advisory/ cpuoct20 17- 3236626. html	COMMO- 011117/ 116
Communicatio	ns Policy Man	agemen			<u>I</u>
NA	19-10-2017	5.8	VulnerabilityintheOracleCommunicationsPolicyManagement component of OracleCommunicationsApplications(subcomponent:Portal,CMP).Supportedversionsthataffected are11.5and12.x.ExploitablevulnerabilityallowsunauthenticatedattackerwithnetworkaccessviaHTTPtocompromiseOracleCommunicationsPolicy	http://w ww.oracl e.com/tec hnetwork /security- advisory/ cpuoct20 17- 3236626. html	A-ORA- COMMU- 011117/ 117
CV Scoring Scale (C	VSS)	0-1	1-2 2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10
Vulnerability Type CSRF-Cross Site Rec Injection; XSS- Cros	quest Forgery; Dir	. TravDir	rectory Traversal; DoS-Denial of Service; NA- N	ot Applicable; S	ql-SQL

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Communication		sion Co	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		
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://w ww.oracl e.com/tec hnetwork /security- advisory/ cpuoct20 17- 3236626. html	A-ORA- COMMU- 011117/ 118

Patch NCII	IPC ID
http://w A-OI ww.oracl COR e.com/tec 0113 network 119 'security- advisory/ cpuoct20 7- 8236626. html	REI- 117/
nnetwork 120 /security- ndvisory/ cpuoct20 17- 3236626. ntml	TO- 117/
7-8 8-9	9-10
App	7-8 8-9 licable; Sql-SQL

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
	bute		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://w ww.oracl e.com/tec hnetwork /security- advisory/ cpuoct20 17- 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://w ww.oracl e.com/tec hnetwork /security- advisory/ cpuoct20 17- 3236626. html	A-ORA- DATAB- 011117/ 122
CV Scoring Scale (CV	VSS)	0-1	1-2 2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Type(s)	Date									
			data or o Databas This s platform Databas version score is CVSS (Confide Vector: (CVSS:3. S:C/C:H)	orized acc complete a e accessil core is n version e. For Wi 12.1.0.2 5.5 with so 3.0 Bas entiality .0/AV:L/A /I:N/A:N).	for M for M n 11.2 ndows and Li cope Un e Sco impacts C:L/PR:	o all XM a. Not Windov 2.0.4 platfor nux, tl change ore 6). CV L/UI:N	AL te: ws of m he ed. 5.5 SS			
NA	19-10-2017	4.3	Vulnera compon Server. are affe and 12 vulneral privilege Session, privilege infrastru Execute VM. Wh Java VM impact Successf vulneral takeove Score Integrity CVSS (CVSS:3. S:C/C:H	bility in ent of C Supported cted are 1 .2.0.1. Ea bility ed attacke Creat e with ucture w utes to co tile the vu attacks r additio ful atta	the J pracle 1 versic 1.2.0.4, sily ex allows r havin e P logon here J ompron lnerabi nal j cks c n res M. CVSS (Confid ability	ava V Databa Databa Databa Databa 12.1.0 ploitab hig g Crea rocedu to the ava V dise Ja ificant oroduc of the sult 3.0 Ba entialite mpacts Vecto H/UI:N	se ww at e.c 0.2 hn ole /se gh ad te cp re 17 he 32 M ht va in cly ts. iis in se ty, s). or:	36626.	A-OR DATA 0111 123	AB-
NA	19-10-2017	4.6	compon Server. are affe and 12 vulneral attacker privilege	bility in t ent of C Supported cted are 1 .2.0.1. Ea bility allow having e with acture who	racle l versi 1.2.0.4, sily ex vs low p Create logon	Databa ons th 12.1.0 ploitab rivilego sessio to th	se ww at e.c 0.2 hn ole /so ed ad on cp he 17	tp://w w.oracl com/tec etwork ecurity- visory/ uoct20 - 36626.	A-OR DATA 0111 124	AB-
CV Scoring Scale (CV Vulnerability Type(s	-	0-1	1-2 2	-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10

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).	html	
E-business Suite	a Tachnology	Stack	CVE ID : CVE-2017-10321		
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://w ww.oracl e.com/tec hnetwork /security- advisory/ cpuoct20 17- 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://w ww.oracl e.com/tec hnetwork /security-	A-ORA-E- BUS- 011117/ 126
CV Scoring Scale (CV	766)	0-1	1-2 2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE	EID	Pate	ch	NCIIPO	D
			attacks of this vulneral result in unauthorized insert or delete access to Oracle Applications Te Stack accessible data. Base Score 5.3 (Integrity CVSS (CVSS:3.0/AV:N/AC:L/PR S:U/C:N/I:L/A:N).	d 12.2.7. nerability attacker HTTP to plications Successful pility can update, o some of echnology CVSS 3.0 impacts). Vector: ::N/UI:N/	advisc cpuoc 17- 32366 html	t20		
Flexcube Unive	weal Danking		CVE ID : CVE-2017-1006	6				
NA	19-10-2017	5.5	(subcomponent: Supported versions t affected are 11.3, 11.4. 12.0.2, 12.0.3, 12.1.0, 12.2 and 12.4.0. Easily ex vulnerability allows low p attacker with network a HTTP to compromise FLEXCUBE Universal Successful attacks vulnerability can re unauthorized access to data or complete access	Banking Financial plications Security). that are 0, 12.0.1, 2.0, 12.3.0 xploitable privileged access via e Oracle Banking. of this esult in p critical ss to all Universal as well as insert or of Oracle Banking Contact 3.0 Base lity and S Vector:	http:// ww.or e.com, hnetw /secur advisc cpuoc 17- 32366 html	racl /tec rork rity- ory/ t20	A-ORA FLEXC 01111 127	-
CV Scoring Scale (C	VSS)	0-1	1-2 2-3 3-4 4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type CSRF-Cross Site Rec Injection; XSS- Cros	quest Forgery; Dir	. TravDir	ectory Traversal; DoS-Denial of S	ervice; NA- N	ot Applic	able; So	ql-SQL	

Vulnerability	Publish	CVSS		Desc	ription	n & CVE	EID		Patch	NCIII	PC ID
Type(s)	Date		CVE	' ID - CI	/E 201	7-1036	2				
Classfish Serve	r		LVE		E-201	/-1030	05				
<u>Glassfish Serve</u> NA	r 19-10-2017	5.8	Glass Orac (sub Graj sup) is vuln unat netv com Serv hum othe atta resu inse Orac data acce Glass CVS (Con imp (CVS	cle pocompo phical ported 3.1.2. herabilit uthenti work promis ver. Such an inte er than cks of alt in cks of alt in cle Glas a as we ess to ssFish S S 3.0 hfidenti acts). SS:3.0/A /C:L/I:L	Server Fusion nent: User version Eas ty cated access access the att this v unaut elete a sFish S ll as un a su Server Bas ality CV AV:N/A (A:N).	comp Mi Admi Interfa n that i ily e attack via l cacle l attack n from cacker. S vulneral horized ccess to Server a nauthor ibset c access se Sc and VSS AC:L/PR	HTTP t GlassFis s requir a perso Successfu pility ca update some c accessible ized rea of Oracl ible data ore 5. Integrit Vector	of w re e.a n hr re /s d ac rs 17 h 32 rs 17 rs 1	tp://w w.oracl com/tec network security- lvisory/ ouoct20 7- 236626. cml	A-OR GLAS 0111 128	S-
DoS	19-10-2017	6.8	Vulr Glas Orac (sub Supj affec expl unat netv com Serv hum othe atta resu inse	nerabili ssFish cle pocompo ported cted ard loitable uthenti work apromis ver. Suc nan inte er than cks of alt in ert or d	ty ir Server Fusion nent: vers e 3.0.1 vuln cated access e Or ccessfu eraction the att this v unaut elete a	h the comp Web C ions t and 3.1 erability attack via l cacle l attack n from cacker. S vulneral horized ccess to	Oracl onent o ddlewar ontainer hat ar l.2. Easil y allow	of w e e.e.). hr e /s y ac y ac y ac y ac y ac y ac y ac y ac	tp://w w.oracl com/tec network security- lvisory/ puoct20 7- 236626. cml	A-OR GLAS 0111 129	S-
CV Scoring Scale (CV	VSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(CSRF-Cross Site Req Injection; XSS- Cross	(s): Juest Forgery; Dir	. TravDir	ectory	v Travers	al; DoS-D	Denial of S	Service; NA	- Not A	pplicable;	Sql-SQL	

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://w ww.oracl e.com/tec hnetwork /security- advisory/ cpuoct20 17- 3236626. html	A-ORA- GLASS- 011117/ 130
DoS	19-10-2017	7.5	Vulnerability in the Oracle GlassFish Server component of Oracle Fusion Middleware	http://w ww.oracl e.com/tec	A-ORA- GLASS- 011117/
			(subcomponent: Administration). Supported versions that are	hnetwork /security-	131
		0-1	1-2 2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

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/ cpuoct20 17- 3236626. html	
Global Order Pa	romising 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://w ww.oracl e.com/tec hnetwork /security- advisory/ cpuoct20 17- 3236626. html	A-ORA- GLOBA- 011117/ 132
	1		contraction of and	I	1

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 Cru				P	1
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://w ww.oracl e.com/tec hnetwork /security- advisory/ cpuoct20 17- 3236626. html	A-ORA- HOSPI- 011117/ 133
Hospitality Cru	ise Fleet Man	agemen	t		
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://w ww.oracl e.com/tec hnetwork /security- advisory/ cpuoct20 17- 3236626. html	A-ORA- HOSPI- 011117/ 134
CV Scoring Scale (C	vss)	0-1	1-2 2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10
Vulnerability Type	(s): Juest Forgery; Dir	. TravDir	rectory Traversal; DoS-Denial of Service; NA- N	ot Applicable; S	ql-SQL

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
DoS	Date	3.5	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 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	http://w ww.oracl e.com/tec hnetwork /security- advisory/ cpuoct20 17- 3236626. html	A-ORA- HOSPI- 011117/ 135
			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		
		0-1	1-2 2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

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).	http://w ww.oracl e.com/tec hnetwork /security- advisory/ cpuoct20 17- 3236626. html	A-ORA- HOSPI- 011117/ 136
NA	19-10-2017	5.8	CVE ID : CVE-2017-10395VulnerabilityintheOracleHospitalityCruiseFleetManagement component of OracleHospitalityApplications(subcomponent: BaseMasterPage).The supported version that isaffectedis9.0.2.0.EasilyexploitablevulnerabilityallowsunauthenticatedattackerwithnetworkaccessviaHTTPcompromiseOracleHospitalityCruiseFleetManagement.Successful attacksrequire humaninteractionfrom a person otherthan the attacker and while thevulnerabilityisinOracleHospitalityKanagement,attacksmaysignificantlyimpactadditional	http://w ww.oracl e.com/tec hnetwork /security- advisory/ cpuoct20 17- 3236626. html	A-ORA- HOSPI- 011117/ 137
CV Scoring Scale (C	-	0-1	1-2 2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10
Vulnerability Type CSRF-Cross Site Rec Injection; XSS- Cros	quest Forgery; Dir	. TravDir	rectory Traversal; DoS-Denial of Service; NA- N	ot Applicable; S	ql-SQL

Vulnerability Type(s)	Publish Date	CVSS	Descri	ption & (CVE ID		Ра	itch	NCI	PC ID
			products. Suc vulnerability unauthorized delete acces Hospitality Management well as unau to a subset Cruise F accessible d Score 6.1 Integrity im (CVSS:3.0/AV S:C/C:L/I:L/A CVE ID : CVE	can l update s to som Cruis accessil ithorized of Oracle leet lata. CVS (Confiden pacts). C /:N/AC:L, A:N).	result e, insert ne of Ora se F ble data read acc e Hospita Managem SS 3.0 E ntiality CVSS Vec /PR:N/UI	in or acle leet as cess ality hent Base and tor:				
Hospitality Cru	ise Materials	Manage	ement						<u>.</u>	
NA	19-10-2017	3.6	Successful vulnerability unauthorized delete access Hospitality Management well as unau to a subset	Cruise component: M ersion tha 0. Easily ted att infrastru tality Cru Exect Oracle cerials M attacks can d update s to som Cruise accessil thorized of Oracle terials (Confider pacts). C <i>Y</i> :L/AC:L/ A:N).	Mater ent of Ora Application IMS). at is affect exploitation acker volucture which ise Mater acker volucture which ise Mater acker volucture which ise Mater acker volucture acker	acle ions The cted able ows with nere rials to ality ent. this in or acle rials as cess ality nent Base and ctor:	ww.e e.con hnet /sec advi cpuc 17-	://w oracl m/tec work urity- sory/ oct20 6626.	A-OI HOS 0111 138	
NA	19-10-2017	4.3	Vulnerability	in t	the Ora	acle	http	.//w	A-OI	₹ A-
CV Scoring Scale (CV	VSS)	0-1	1-2 2-3	3-4 4	-5 5-6	6	5-7	7-8	8-9	9-10
Vulnerability Type(CSRF-Cross Site Req Injection; XSS- Cros	quest Forgery; Dir	. TravDir	ectory Traversal;	DoS-Denial	of Service;	NA- No	ot Appl	icable; S	Sql-SQL	

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
736-(3)			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 cru 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).	ww.oracl e.com/tec hnetwork /security- advisory/ cpuoct20 17- 3236626. html	HOSPI- 011117/ 139
			CVE ID : CVE-2017-10401		
Hospitality Cru DoS	<u>tise Shipboard</u> 19-10-2017	5.5	<i>ty Management System</i> 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://w ww.oracl e.com/tec hnetwork /security- advisory/ cpuoct20 17-	A-ORA- HOSPI- 011117/ 140
CV Scoring Scale (C	VSS)	0-1	1-2 2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10
Vulnerability Type((s): quest Forgery; Dir	. TravDii	rectory Traversal; DoS-Denial of Service; NA- N	ot Applicable; S	ql-SQL

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 10261	3236626. html	
Hospitality Gue	ast Accass		CVE ID : CVE-2017-10361		
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://w ww.oracl e.com/tec hnetwork /security- advisory/ cpuoct20 17- 3236626. html	A-ORA- HOSPI- 011117/ 141
CV Scoring Scale (C	VSS)	0-1	1-2 2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10
Vulnerability Type(CSRF-Cross Site Rec Injection; XSS- Cros	quest Forgery; Dir	. TravDir	ectory Traversal; DoS-Denial of Service; NA- N	ot Applicable; S	Gql-SQL

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://w ww.oracl e.com/tec hnetwork /security- advisory/ cpuoct20 17- 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://w ww.oracl e.com/tec hnetwork /security- advisory/ cpuoct20 17-	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://w ww.oracl e.com/tec hnetwork /security- advisory/ cpuoct20 17- 3236626. html	A-ORA- HOSPI- 011117/ 144
Hospitality Hot	tel Mobile			Γ	I
NA	19-10-2017	3.5	VulnerabilityintheOracleHospitalityHotelMobilecomponentofOracleHospitality	http://w ww.oracl e.com/tec	A-ORA- HOSPI- 011117/
CV Scoring Scale (CV	VSS)	0-1	1-2 2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10
Vulnerability Type((s): quest Forgery; Dir	. TravDir	ectory Traversal; DoS-Denial of Service; NA- N	ot Applicable; S	ql-SQL

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID Patch NCIIPC ID
			Applications(subcomponent: suite8/RESTAPI). The supported /security- version that is affected is 1.1. advisory/ Easily exploitable vulnerability allows low privileged attacker
DoS	19-10-2017	5.5	VulnerabilityintheOraclehttp://wA-ORA-HospitalityHotelMobileww.oraclHOSPI-component of Oracle Hospitalitye.com/tec011117/Applications(subcomponent:hnetwork146Suite8/RESTAPI).The supported/security-version that is affected is 1.1.advisory/Easilyexploitablevulnerabilitycpuoct20allowslowprivilegedattacker17-with network access viaHTTP to3236626.htmlcompromiseOracleHospitalityhtmlHotel Mobile.Successful attacks ofhtmlHotel Mobile.Success tocriticaldataorcompleteaccessdataorcompleteaccessdataorcompleteaccessdataorcompleteaccessdataorcompleteaccessibledataandabilityto cause a partial denial ofservice(partialDOS)BaseScore 7.1(Confidentiality andAvailabilityimpacts).CVS3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:L).CVE ID : CVE-2017-10353
Hospitality Ope			
Gain	19-10-2017	2.1 0-1	Vulnerability in the Oracle http://w A-ORA- 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10
CV Scoring Scale (CV			

Vulnerability	Publish	CVSS	Description & CVE IDPatchNCIIPC
Type(s) Information	Date		Hospitality OPERA 5 Property Services component of Oracle Hospitalityww.oracl e.com/tecHOSPI-
			CVE ID : CVE-2017-10197
Hospitality Rep			
NA	19-10-2017	4.6	VulnerabilityintheOraclehttp://wA-ORA-HospitalityReportingandww.oraclHOSPI-Analyticscomponentof Oraclee.com/tec011117,HospitalityApplicationshnetwork148(subcomponent:iQuery).Security-advisory/Supportedversionsthatareaffectedare8.5.1and9.0.0.Difficulttoexploitvulnerabilityallowslowprivilegedattackerwith networkaccess viaHTTPtocompromiseOracleHospitalityReportingandAnalytics.Successfulattacksrequire humaninteractionfrom a person otherthantheattacksvulnerabilityisinOracleHospitalityimpactadditionalproducts.SuccessfulattacksvulnerabilitycanresultintakeoverofOracleHospitalityReportingandAnalytics.CVSS 3.0BaseScoreBaseScore12344556677889
CV Scoring Scale (CV	-	0-1	1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9
Vulnerability Type(CSRF-Cross Site Req Injection; XSS- Cross	quest Forgery; Dir	. TravDir	irectory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL

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	VulnerabilityintheOracleHospitalityReportingandAnalyticscomponentofOracleHospitalityApplications(subcomponent:Report).Supportedversionsthatareaffected are8.5.1 and9.0.0.EasilyexploitablevulnerabilityallowsunauthenticatedattackerwithnetworkaccessviaHTTPtocompromiseOracleHospitalityReportingandAnalytics.While thevulnerabilityisinOracleHospitalityReportingandAnalytics, attacksmay significantlyimpactadditionalproducts.SuccessfulattacksofthisvulnerabilitycanresultinunauthorizedaccesstoallOracleHospitalityReportingandAnalyticsaccesssuccessibledataandunauthorizedabilitytocauseaandunauthorizedabilitytocauseaandAnalytics.CVSS3.0BaseScore10.0(ConfidentialityandAnalytics.CVSS3.0BaseScore10.0(ConfidentialityandAvailabilityimpacts).CVSS Vector:(CVSS:3.0/AV:N/AC:L/PR:N/UI:N/ <td< td=""><td>ww.oracl e.com/tec hnetwork /security- advisory/ cpuoct20 17- 3236626. html</td><td>A-ORA- HOSPI- 011117/ 149</td></td<>	ww.oracl e.com/tec hnetwork /security- advisory/ cpuoct20 17- 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	ww.oracl e.com/tec hnetwork /security- advisory/ cpuoct20 17-	A-ORA- HOSPI- 011117/ 150
CV Scoring Scale (C	VSS)	0-1	1-2 2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10
Vulnerability Type CSRF-Cross Site Rec Injection; XSS- Cros	quest Forgery; Dir	. TravDii	ectory Traversal; DoS-Denial of Service; NA- I	Not Applicable; S	Gql-SQL

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
NA	19-10-2017	7.5	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 Vulnerability in the Oracle Hospitality Reporting and Analytics component of Oracle Hospitality Reporting and Analytics withe the vulnerability in the Oracle Hospitality Reporting and Analytics, attacks 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).	html html http://w ww.oracl e.com/tec hnetwork /security- advisory/ cpuoct20 17- 3236626. html	A-ORA- HOSPI- 011117/ 151
Hospitality Sim	nphony		CVE ID : CVE-2017-10402		
Gain Information	19-10-2017	4.3	Vulnerability in the Oracle Hospitality Simphony component	http://w ww.oracl	A-ORA- HOSPI-
CV Scoring Scale (C	VSSI	0-1		6-7 7-8	8-9 9-10
Vulnerability Type	(s): quest Forgery; Dir	. TravDir	rectory Traversal; DoS-Denial of Service; NA- N	ot Applicable; S	ql-SQL

Vulnerability	Publish Date	CVSS	Desc	ription & CV	E ID	P	atch	NCII	PC ID
<u>Type(s)</u>	Date		(subcompor Supported affected ar exploitable unauthentic network a compromise Simphony. require hur person oth Successful vulnerabilit unauthorize data or co Oracle H accessible Score 6 impacts). (CVSS:3.0/A S:U/C:H/I:N	e 2.8 and 2 vulnerabilit ated attack ccess via e Oracle H Successful nan interacti er than the attacks y can r ed access t omplete acce ospitality data. CVSS 5.5 (Conf CVSS	t/Export). that are 2.9. Easily ty allows ker with HTTP to Hospitality attacks on from a attacker. of this esult in to critical ess to all Simphony 3.0 Base identiality Vector: R:N/UI:R/	hne /se adv cpu 17- 323 htm	86626.	0111 152	.17/
NA	19-10-2017	5.5	Vulnerabilit Hospitality of Oracle H (subcompor Supported affected are Easily exp allows low with netwo compromise Simphony. this vulner unauthorize delete acce Hospitality data as wel access to Hospitality data. CVSS (Confidentia impacts). (CVSS:3.0/A S:U/C:L/I:L	y in the Simphony c lospitality Appendix Service versions 2.6, 2.7, 2.3 oloitable vu y privileged rk access via e Oracle H Successful a rability can ed update, ss to some Simphony l as unautho a subset Simphony 3.0 Base ality and CVSS AV:N/AC:L/Pl	e Oracle omponent oplications ce Host). that are 8 and 2.9. Inerability attacker a HTTP to Hospitality attacks of result in insert or of Oracle accessible rized read of Oracle accessible Score 5.4 Integrity Vector: R:L/UI:N/	ww e.cc hne /se adv cpu 17- 323 htm	86626.	A-OR HOSI 0111 153	PI-
CV Scoring Scale (CV	VSS)	0-1	1-2 2-3	3-4 4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(CSRF-Cross Site Req Injection; XSS- Cros	uest Forgery; Dir	. TravDir	ectory Traversa	l; DoS-Denial of	Service; NA-	Not App	plicable; S	Sql-SQL	

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).	http://w ww.oracl e.com/tec hnetwork /security- advisory/ cpuoct20 17- 3236626. html	A-ORA- HOSPI- 011117/ 154
NA	19-10-2017	5.8	CVE ID : CVE-2017-10367VulnerabilityintheOracleHospitalitySimphonycomponentofOracleHospitalityApplications(subcomponent:Import/Export).Supportedversionsthataffected are2.8 and2.9.Difficult toexploitvulnerabilityallowsunauthenticatedattackerwithnetworkaccessviaHTTPtocompromiseOracleHospitalitySimphony.SuccessfulattacksofthisvulnerabilitycanresultunauthorizedaccesstocriticaldataorcompleteaccesstoOracleHospitalitySimphonyaccessibleataunauthorizedupdate,insertordeleteaccesstosome ofOracleHospitalitySimphonyaccessibleaccessible	http://w ww.oracl e.com/tec hnetwork /security- advisory/ cpuoct20 17- 3236626. html	A-ORA- HOSPI- 011117/ 155
CV Scoring Scale (C	VSS)	0-1		6-7 7-8	8-9 9-10
Vulnerability Type CSRF-Cross Site Rec Injection; XSS- Cros	quest Forgery; Dir	. TravDir	ectory Traversal; DoS-Denial of Service; NA- N	ot Applicable; S	ql-SQL

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://w ww.oracl e.com/tec hnetwork /security- advisory/ cpuoct20 17- 3236626. html	A-ORA- HOSPI- 011117/ 156
Hospitality Sui	te8		CVE ID : CVE-2017-10340		
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://w ww.oracl e.com/tec hnetwork /security- advisory/ cpuoct20 17- 3236626. html	A-ORA- HOSPI- 011117/ 157
CV Scoring Scale (C	VSS)	0-1	1-2 2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10
Vulnerability Type CSRF-Cross Site Rec Injection; XSS- Cros	quest Forgery; Dir	. TravDir	ectory Traversal; DoS-Denial of Service; NA- N	ot Applicable; S	ql-SQL

Vulnerability Type(s)	Publish Date	CVSS		Descri	ption	& CVE	ÎD		Patch	۱ I	NCIIP	C ID
	bute		result to a Suite Base impa- (CVSS S:U/O	ks of t t in una subset 8 acces Score cts). 5:3.0/AV C:L/I:N/ D : CVE	uthor of Or sible 4.0 CV /:L/A(A:N).	ized re acle H data. (Confi SS C:L/PR	ad acce ospital CVSS 3 dential Vecto :N/UI:N	ess ity 3.0 ity or:				
NA	19-10-2017	3.6	Hosp Oracl (subc versic 8.10.7 explo unaut logom Oracl Execu Hosp attacl result inser Oracl acces unaut subse acces Score Integ (CVSS S:U/O	itable thentica to the e H iteutes itality ks of t t in u t or del e H	Suite8 pitalit ent: P at ar d { vulne ited infras Hospit to con Suite his vu nauth ete ac Hospit data l rea acle H lata. (Conf pacts) <i>I</i> :L/AC A:N).	comp y Ap MS). S e affe 3.10.2. rability attack structu ality nprom e8. S ulneral corized ccess to ality as d acce ospital CVSS identia . CVSS C:L/PR	oonent plicatio cupport cted a Eas y allow er whe Suit re whe Suit ise Orac Success oility c upda o some Suit well ess to ity Suit 3.0 Ba llity a S Vecto :N/UI:N	of v ons e ed h ire / ily a ws c ith 1 ere 3 ith 1 ere 4 ith 1 ere 3 ith 1 e 1 e i 1 e i i i i i i i i i i i i i	uttp://v vw.orac e.com/tu inetwor securit idvisory puoct2 .7- 323662 utml	cl l ec (rk f y- y/ 0	A-ORA HOSPI 01111 158	[-
Gain Information	19-10-2017	4	Hosp Oracl (subc Supp affect Easily allow with comp Suite	erability itality s ompon- orted red are y expl rs low networ romise 8. Succi- prability	Suite8 pitalit ent: versio 8.10 oitablo priv k acco Ora essful	comp y Ap ons t 0.1 an e vul ileged ess via cle H attack	plicatio Leisur hat a d 8.10 nerabil attack HTTP ospital	of v ons e e). h are / 0.2. a ity c ter 1 to 3 ity h	e.com/te e.com/te inetwor securit idvisory puoct2 7- 23662 itml	cl l ec (rk f y- y/ 0	A-ORA HOSPI 01111 159	[-
CV Scoring Scale (CV	700)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	3	8-9	9-10

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://w ww.oracl e.com/tec hnetwork /security- advisory/ cpuoct20 17- 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://w ww.oracl e.com/tec hnetwork /security- advisory/ cpuoct20 17- 3236626. html	A-ORA- HOSPI- 011117/ 161
CV Scoring Scale (CV		0-1	1-2 2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID Patch NCIIPC ID
<u>1 ype(5)</u>			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	VulnerabilityintheOraclehttp://wA-ORA-HospitalitySuite8component ofww.oraclHOSPI-OracleHospitalityApplicationse.com/tec011117/(subcomponent:WebConnect).hnetwork162Supportedversionsthatare/security-affectedare8.10.1and8.10.2.advisory/Difficulttoexploitvulnerabilitycpuoct20allowsunauthenticatedattacker17-withnetworkaccess viaHTTP3236626.compromiseOracleHospitalityhtmlSuite8.Successfulattacks ofhtmlSuite8.Successfulattacks ofhtmlunauthorizedaccesstoalloracleHospitalitySuite8accessibleaccessibledata.CVSS3.0BaseScore5.9(Confidentiality)impacts).CVSSVector:(CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N).CVE ID:CVE-2017-10339
Gain Information	19-10-2017	4.3	VulnerabilityintheOraclehttp://wA-ORA-HospitalitySuite8component ofww.oraclHOSPI-OracleHospitalityApplicationse.com/tec011117/(subcomponent:WebConnect)hnetwork163Supportedversionsthatare/security-affectedare8.10.1and8.10.2.advisory/Easilyexploitablevulnerabilitycpuoct20
CV Scoring Scale (C	-	0-1	1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10
Vulnerability Type(CSRF-Cross Site Rec Injection; XSS- Cros	quest Forgery; Dir	. TravDir	rectory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL

Vulnerability	Publish	CVSS	Description & CVE ID	Patch	NCIIPC ID
Type(s) Gain Information	Date	5	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 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. Successful attacks of this vulnerability can result in unauthorized read access to a subset of 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).	17- 3236626. html http://w ww.oracl e.com/tec hnetwork /security- advisory/ cpuoct20 17- 3236626. html	A-ORA- HOSPI- 011117/ 164
DoS	19-10-2017	5.5	CVE ID : CVE-2017-10319VulnerabilityintheOracleHospitalitySuite8componentofOracleHospitalityApplications(subcomponent:Leisure).Supportedversionsthataffectedare8.10.1andEasilyexploitablevulnerability	http://w ww.oracl e.com/tec hnetwork /security- advisory/ cpuoct20	A-ORA- HOSPI- 011117/ 165
CV Scoring Scale (CV Vulnerability Type(CSRF-Cross Site Req Injection; XSS- Cros	(s): quest Forgery; Dir	0-1 . TravDir	1-22-33-44-55-6ectory Traversal; DoS-Denial of Service; NA- N	6-7 7-8 ot Applicable; S	8-9 9-10 ql-SQL

Vulnerability	Publish	CVSS	Description & CVE ID	Patch	NCIIPC ID
Type(s)	Date		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).	17- 3236626. html	
DoS Gain Information	19-10-2017	5.5	CVE ID : CVE-2017-10420 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://w ww.oracl e.com/tec hnetwork /security- advisory/ cpuoct20 17- 3236626. html	A-ORA- HOSPI- 011117/ 166
NA	19-10-2017	5.8	VulnerabilityintheOracleHospitalitySuite8componentofOracleHospitalityApplications	http://w ww.oracl e.com/tec	A-ORA- HOSPI- 011117/
		0-1	1-2 2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQI Injection; XSS- Cross Site Scripting;

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/ cpuoct20 17- 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://w ww.oracl e.com/tec hnetwork /security- advisory/ cpuoct20 17- 3236626. html	A-ORA- HYPER- 011117/ 168
CV Scoring Scale (C	VSS)	0-1	1-2 2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10
Vulnerability Type CSRF-Cross Site Rec Injection; XSS- Cros	quest Forgery; Dir	. TravDir	rectory Traversal; DoS-Denial of Service; NA- N	ot Applicable; S	ql-SQL

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
<u> </u>	Date		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).	http://w ww.oracl e.com/tec hnetwork /security- advisory/ cpuoct20 17- 3236626. html	A-ORA- HYPER- 011117/ 169
Hyperion Finar	ncial Reportin	a	CVE ID : CVE-2017-10312		
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://w ww.oracl e.com/tec hnetwork /security- advisory/ cpuoct20 17- 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(CSRF-Cross Site Req Injection; XSS- Cros	uest Forgery; Dir	. TravDii	ectory Traversal; DoS-Denial of Service; NA- N	lot Applicable; S	Gql-SQL

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID Patch NCIIPO	CID		
Vumerability Type(s) NA	Publish Date	5.5	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-2017-10310http://w A-ORA- 			
			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			
Identity Manag	jer Connector					
NA	19-10-2017	3.3	Vulnerability in the Oracle Identityhttp://wA-ORA-Manager Connector component ofww.oraclIDENT-OracleFusionMiddlewaree.com/tec011112(subcomponent:Microsoft Activehnetwork172Directory).The supported version/security-that is affected is 9.1.1.5.0.Easilyadvisory/exploitablevulnerabilityallowscpuoct20unauthenticatedattackerwith17-	-		
CV Scoring Scale (CV	VSS)	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. TravDirectory 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
			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
Interaction Cer	nter Intelligen	ice	
NA	19-10-2017	5.8	VulnerabilityintheOraclehttp://wA-ORA-InteractionCenterIntelligenceww.oraclINTER-componentofOracleE-Businesse.com/tec011117/Suite(subcomponent:Setup).hnetwork173Supportedversionsthatare/security-affectedare12.1.1,12.1.2andadvisory/12.1.3.Easilyexploitablecpuoct20vulnerabilityallows17-unauthenticatedattackerwithnetworkaccessviaHTTPtocompromiseOracleInteractionCenterfrom a person otherthan theattackerandwhilethevulnerabilityisinOracleInteractionCenterfrom a person otherthan theattacksmay significantly impactattacksmay significantly impactadditionalproducts.Successful
CV Scoring Scale (C		0-1	1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10
Vulnerability Type CSRF-Cross Site Rec Injection; XSS- Cros	quest Forgery; Dir	. TravDir	irectory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL

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 Se	rver				
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://w ww.oracl e.com/tec hnetwork /security- advisory/ cpuoct20 17- 3236626. html	A-ORA- IPLAN- 011117/ 174
Istore					
CV Scoring Scale (C	VSS)	0-1	1-2 2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10
Vulnerability Type(CSRF-Cross Site Rec		. TravDir	ectory Traversal; DoS-Denial of Service; NA- N	ot Applicable; S	ql-SQL

CSRF-Cross Site Request Forgery; Dir. Trav.-Directory 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://w ww.oracl e.com/tec hnetwork /security- advisory/ cpuoct20 17- 3236626. html	A-ORA- ISTOR- 011117/ 175
NA	19-10-2017	5.8	CVE ID: CVE-2017-10414Vulnerability in the Oracle iStore component of Oracle E-BusinessSuite (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://w ww.oracl e.com/tec hnetwork /security- advisory/ cpuoct20 17- 3236626. html	A-ORA- ISTOR- 011117/ 176
CV Scoring Scale (C	-	0-1	1-2 2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10
Vulnerability Type CSRF-Cross Site Rec Injection; XSS- Cros	quest Forgery; Dir	. TravDir	ectory Traversal; DoS-Denial of Service; NA- N	ot Applicable; S	ql-SQL

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE IDPatchNCIIPC 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	VulnerabilityintheOraclehttp://wA-ORA-iSupport component of Oracle E-ww.oraclISUPP-BusinessSuite (subcomponent:e.com/tec011117/Others).Supported versions thathnetwork177areaffected are12.1.1,12.1.2,/security-12.1.3,12.2.3,12.2.4,12.2.5,12.2.6advisory/and12.2.7.Easilyexploitablecpuoct20vulnerabilityallows17-unauthenticatedattackerwithnetworkaccessviaHTTPtoompromiseOracleiSupport,successfulattacksrequire humaninteraction from a person otherthantheattacker and while thevulnerability is in Oracle iSupport,attacksattacksattacks of this vulnerability canresult in unauthorized access toall Oracle iSupport accessible dataasas well as unauthorized update,insert or delete access to some ofOracle iSupport accessible data.CVSS3.0BaseScoreS:C/C:H/I:L/A:N).CVE ID:CVE-2017-10415
Java Advanced	Management		
CV Scoring Scale (CV	VSS)	0-1	1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10
Vulnerability Type CSRF-Cross Site Rec Injection; XSS- Cros	quest Forgery; Dir	. TravDii	rectory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL

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 advisory/
NA	19-10-2017	4.3	Vulnerability in the Java Advancedhttp://wA-ORA-Management Console componentww.oraclJAVA -of Oracle Java SE (subcomponent:e.com/tec011117/Server). The supported versionhnetwork179that is affected is Java Advanced/security-Management Console: 2.7. Difficultadvisory/to exploit vulnerability allowscpuoct20unauthenticatedattacker with17-attackernetworkaccess via multiple3236626.htmlSuccessfulattacksvulnerabilitycanunauthorizedupdate, insert orunauthorizedupdate, insert or
CV Scoring Scale (C	VSS)	0-1	1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10
Vulnerability Type CSRF-Cross Site Rec Injection; XSS- Cros	quest Forgery; Dir	. TravDii	rectory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL

Vulnerability Type(s)	Publish Date	CVSS	Des	cription	& CVE	E ID		Patch	NCI	IPC ID
			delete ac Advanced accessible vulnerabil deployme running sa applicatio applets, untrusted comes fro on the Ja This vuln to Java d servers, t trusted co by an ac Base Scor CVSS (CVSS:3.0, S:U/C:N/I	Manag data. ity apj nts, typi andboxed ns or s that lo code (m the in va sandb erability eployme hat load ode (e.g. lministra e 3.7 (Int /AV:N/A	ement Not plies cally i d Java V sandbo oad a (e.g., c ternet) oox for does 1 nts, ty l and , code ator). tegrity C:H/PF	Conso e: Th to Jay mode th and ru ode th and re securit not app pically run on installe CVSS 3 impacts Vecto R:N/UI:N	le lis va ts rt va n at ly yy. ly in ly ed .0 5). or:			
NA	19-10-2017	4.9	CVE ID : C Vulnerabi Managem of Oracle Sever). Th is affecto Managem exploitabl high pri network comprom Managem attacks re from a p attacker vulnerabil Managem significant products. vulnerabil unauthori delete ac Advanced accessible unauthori subset	lity in the ent Cons Java SE e suppored is ent Cons e vulne vileged access ise Ja ent Cons quire hu person of and ity is in ent Cons cly imp Successfi ity ca zed upo cess to Manag data zed rea	e Java A sole co (subco cted ve Java A sole: 2 erability attack via I va A sole: 5 man ir other Whi Java A ole, attac n re date, i some ement as d acce	Advance omponer rsion th Advance .7. Easi y allov cer wir HTTP Advance Successf iteractic than th le th Advance cacks ma addition cks of th esult nsert of Jav Conso well	nt ww nt: e.c at hm ed /s ly ad vs cp th 17 to 32 ed ht on ne ed ay al is in or va le as a	36626.	A-0 JAV 011 180	
CV Scoring Scale (C	_	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. TravDirectory 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
<u></u>			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	3	
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 (partia 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	t ww.oracl e.com/tec hnetwork /security- advisory/ cpuoct20 17- 23236626. 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 tha 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	t ww.oracl e.com/tec hnetwork /security- advisory/ cpuoct20 e 17- s 3236626. html	A-ORA- JDK;J- 011117/ 182
		0-1	1-2 2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Vulnerability Type(s)	Publish Date	CVSS	De	scriptior	ı & CVE	ID		Patch	NCI	IPC ID
			unauthor data or co SE, Java accessible vulnerabi through s applicatio applets. I supplying specified using san applicatio applets, service. 0 (Confider Vector: (CVSS:3.0 S:U/C:H/ CVE ID :	omplete a SE Em e data. llity can candboxe ons and t can also g data to Compondboxed ons or such as CVSS 3.0 ntiality p/AV:L/A I:N/A:N).	access t bedded Not be d Java V sandbo o be exp to APIs onent Java W sandbo throug Base S impacts	to all Ja l, JRocl e: Th exploit Web Sta oxed Ja oloited s in t witho Veb Sta xed Ja h a w Score 6 s). CV :N/UI:N	kit his art iva by the out art iva reb 6.2 TSS			
NA	19-10-2017	4	Vulnerab compone (subcomp Supporte affected 7u151, 8 exploit unauthen network protocols Successfu interaction than th attacks of result in deletion critical accessible unauthor data or co SE acces vulnerabi deployme running s application applets, untrusteo	ility in nt of (oonent: S d versi are Jay u144 an vulnera ticated access to comp d attacks on from e attac of this v unauth or modifi data or e data ized acc omplete a sible da lity ap ents, typ andboxe ons or that l	the Oracle Smart (ions t va SE: d 9. Di ability attack via promise s requir a pers vulnerat orized ication r all as cess to access to access to plies bically i ed Java V sandboi load a	Java Java Java Card IG chat a chat a chat a chat a counce ifficult allow multip e Java S cre hum con oth Success Java S creatio access Java well co all Ja cote: Th to Ja in clier Web Sta xed Ja and T	SE w O). e.a are hr 51, /s to ac ws cp ith 17 ole 32 SE. ht an er ful can on, to SE as cal wa his iva his art iva un	ttp://w w.oracl com/tec network security- dvisory/ Duoct20 7- 236626. tml	A-OI JDK; 011 183	;J- 117/
CV Scoring Scale (CV	VSS)	0-1	1-2 2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type CSRF-Cross Site Rec Injection; XSS- Cros	quest Forgery; Dir	. TravDir	ectory Trave	rsal; DoS-D	enial of S	ervice; N	A- Not A	pplicable; S	Sql-SQL	

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID Patch NCIIPC II
			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, Javahttp://wA-ORA-SEEmbeddedcomponentofww.oraclJDK;J-Oracle Java SE(subcomponent:e.com/tec011117/Serialization). Supported versionshnetwork184that are affected are Java SE:/security-6u161, 7u151, 8u144 and 9; Javaadvisory/SEEmbedded:8u144.Embedded:8u144.auvisory/guot20exploitable vulnerability allows17-unauthenticatedattacker withnetworkaccess viamultipleprotocols to compromise Java SE,Java SEEmbedded.Successfulattacks of this vulnerability canresult in unauthorized ability tocause a partial denial of service(partial DOS) of Java SE, Java SEEmbedded.Note:running sandboxed Java Web Startapplications or sandboxed Javaapplets, that load and rununtrusted code (e.g., code thatcomes from the internet) and relyon the Java sandbox for security.This vulnerability does not applyto Java deployments, typically inservers, that load and run onlytrusted code (e.g., code installedby an administrator).CVSSVector:(CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).
CV Scoring Scale (CV	VSS)	0-1	1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-1
Vulnerability Type((s): quest Forgery; Dir	. TravDir	irectory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL

Vulnerability Type(s)	Publish Date	CVSS		Desc	riptior	n & CVE	ID		Patch	NCIIPC ID
Type(3)	Date		CVE	ID : CV	/E-201	7-1035	7			
DoS	19-10-2017	5	Vuln SE Orac JAX- are 8u14 vuln unau netv prot Java attao resu causs (par Emb vuln depl runr appl appl untr com on t This to Ja serv truss by 5 Base impa (CVS S:U/	nerabili Embe Sele Jav WS). S affecte 44 and 44. nerabilif uthenti vork cools t SE cks of lt in u se a pa tial DC bedded. nerabilif oymen ning san ication lets, t custed es from the Java se from the Java custed ers, th ted coo an adu ers, th ted coo an adu con SS:3.0/A	ty in t dded a SE upport d are 9; Jav Easily ty cated access o comp Embed this v unautho artial d OS) of J ty ap ts, typ ndboxe s or chat l code n the ir a sandl rability ployme at load de (e.g ministr re 5. CV AV:N/A V/A:L).	compo (subco ed vers Java SI a SE En attack via oromise ded. S ulneral orized enial c lava SE lenial c lava SE lenial c lava SE ically i d Java V sandbo oad a (e.g., c ternet) oox for chernet) oox for ents, ty d and ., code ator). 3 (Av 7SS	SE, Jay ment mponer sions th E: 7u15 mbedde xploitab allov er wi multip e Java S Guccessf oility ca ability of servic , Java S Guccessf oility ca ability of servic , Java S Th to Jay n clien Web Sta xed Jay and ru ode th and re securit not app pically run on installe CVSS 3 vailabili Vecto :N/UI:N	of www. rat = hm rat = hm rat = hm rat = cp rat = c	36626.	A-ORA- JDK;J- 011117/ 185
DoS	19-10-2017	5	SE Orac JAXE affec 7u1 Emb expl unau	Embe cle Jav ?). Supp cted a 51, 8u oedded: oitable uthenti	dded a SE oorted ire Jav 144 a 8 vulno	compo (subco version va SE:	mponer s that a 6u16 Java S Easi y allov	of ww nt: e.c re hm 1, /s SE ad ly cp vs 17 th 32	36626.	A-ORA- JDK;J- 011117/ 186
CV Scoring Scale (C	VSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9 9-10
Vulnerability Type CSRF-Cross Site Rec Injection; XSS- Cros	(s): quest Forgery; Dir	. TravDir	rectory	Travers	al; DoS-D	enial of S	ervice; NA	A- Not A	pplicable; S	6ql-SQL

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).
DoS	19-10-2017	5	CVE ID : CVE-2017-10349A-ORA-Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Libraries). Supported versions that are affected are Java SE: (security- 6u161, 7u151, 8u144 and 9; Java SE Embedded: 8u144. Easily cpuoct20 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 JavaA-ORA- WW.oracl UDK;J- A-ORA WULRED A-ORA A-ORA WENTOR
CV Scoring Scale (C	vss)	0-1	1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10
Vulnerability Type(CSRF-Cross Site Rec Injection; XSS- Cros	quest Forgery; Dir	. TravDir	rectory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL

Vulnerability Type(s)	Publish Date	CVSS		Desc	ription	1 & CVI	EID		Patch	NCI	IPC ID
			untr com on t This to J serv trus by Base imp (CVS S:U/	es from the Java ava dej rers, th ted coo an adr e Sco acts).	code i the in a sandl rability oloyme at load le (e.g ninistr re 5. CV AV:N/A I/A:L).	(e.g., onternet box for does ents, ty d and ator). .3 (A /SS AC:L/PF	code th) and re securi not app pically run or install CVSS 3 vailabili Vecto CVSS 3	ely ty. oly in hly ed 3.0 ity or:			
DoS	19-10-2017	5	Vulr JRoc SE (Sup) affec 7u1. Emb expl unat netv prot JRoc vuln unat part DOS vuln depl runn appl untr com on t This to J serv trus by Base	nerabilit ckit com subcom ported cted a 51, 8u pedded: oitable uthentio vork cools to ckit. Suc erabilit uthorize ial den) of Jav erabilit loymen ning sar lication lets, t susted es from che Java s vulnen ava dep rers, th ted coo an adr e Sco acts).	y in poner poner versi re Jav 144 a vulne cated access o comp ccessfu y ca ed abi ial of a SE, JF y ap ts, typ ndboxe s or hat l code n the in a sandl rability ployme at load at load	the nt of O nt: Seri ions 5 va SE nd 9; u144. erabilit attack via promise attack ically to servic cockit. 1 plies ically d Java sandbo load 5 (e.g., o ternet box for does ents, ty d and s, code ator). .3 (A /SS	Java S racle Ja alization that a that a Java S Eas y allow ter wi multip e Java S ks of th esult cause e (part Note: Th to Ja in clier Web Sta xed Ja	va w n). e ire h 51, / SE a ily c ily c ily 1 sec c in 3 iel h SE, 5 in a ial nis va 1 sec c in 3 iel h SE, 6 in 1 iel h SE, 6 in 1 iel h SE, 6 in 2 iel h SE, 6 in 1 iel h SE, 6 in 1 iel h SE, 7 in 2 iel h SE, 7 in 1 iel h SE, 1 iel h SE, 1 in 1 i i i i i i i i i i i i i i i i i i i	ttp://w /w.oracl .com/tec network security- dvisory/ puoct20 7- 236626. tml	A-0 JDK 011 188	;J- 117/
CV Scoring Scale (C	VSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type CSRF-Cross Site Rec Injection; XSS- Cros	(s): quest Forgery; Dir	. TravDii	rectory	Traversa	ıl; DoS-D	enial of S	Service; N	A- Not A	Applicable;	Sql-SQI	

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
JT - (-)			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://w ww.oracl e.com/tec hnetwork /security- advisory/ cpuoct20 17- 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	hnetwork	A-ORA- JDK;J- 011117/ 190
CV Scoring Scale (C	VSS)	0-1	1-2 2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10
Vulnerability Type CSRF-Cross Site Rec Injection; XSS- Cros	quest Forgery; Dir	. TravDii	ectory Traversal; DoS-Denial of Service; NA- N	ot Applicable; S	ql-SQL

Type(s)DaNA19	-10-2017	6.8	una sub Not Java clie We san and tha rely sec not typ run inst CVS (Co imp (CV S:C/ CVI Vul SE Ora Hot	authorize oset of Ja te: This y a deplo ents run eb Stan dboxed d run un at comes y on th curity. The tapply oically in n only tr talled b SS 3.0 onfidentia pacts). /SS:3.0/A t/C:L/I:L/ E ID : CV Inerability Embed acle Java tspot). So	ed rea ava SE vulner bymen ining rt a Java a trusted from he Jav he Jav he Jav his vu to Ja serve custed by an Bas ality CV AV:N/A (A:N). E-201 ty in t dded a SE	ad acc E access rability sandbo applicat applets, d code the inte va san ulnerability va dep ers, that code (admini- se Sc and VSS AC:L/PF the Java compo (subco	oxed Java ions on that load (e.g., code ernet) and dbox for ility does oloyments load and (e.g., code nistrator) core 6.1 Integrity Vector R:N/UI:R/ 93 a SE, Java onent of	a a r l e l e l f www : e i i i i i i i i www : e.co	p://w 7.oracl om/tec	A-0 JDK 011 191	
			7u1 Em exp una net pro Java atta fron atta vuli Em sign pro vuli tako Em	151, 8u abedded: oloitable authentic twork a otocols to a SE 1 acks requ m a pe acker acker acker acker acker bedded, nificantly oducts. Su acover co bedded. anerabilit	144 a vuln cated access o com Embec uire hi erson and ty is in and ty is im uccess ty ca of Jav	Java S and 9; Bu144. herabilit attack s via promise dded. S uman in other in Java S attacks pact a sful attac can re va SE, Note: pplies	E: 6u161 Java SE Easily y allows ker with multiple e Java SE Successfu nteractior than the	, /se E adv 7 cpu 5 17- 1 323 e htm , 1 1 2 5 1 5 1 5 1 5 1 5 1 5 1 5 1 5 1 5	36626.		
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											

Vulnerability Type(s)	Publish Date	CVSS		Desci	riptio	n & CV	E ID		F	atch	NC	IPC ID
			appl appl untr come on t This to Ja serve trust by a Base Integ CVSS (CVS S:C/O	S:3.0/A C:H/I:H	or hat code the in sand ability loyme at loa e (e.g ninistr 9.6 d Avai V:N/A /A:H).	sandbo load (e.g., nternet box fo box fo does ents, ty d and g., code ator). (Confi llability	oxed and code) and r secu not a pically run e insta CVSS dentia vimpa Veo R:N/U	Java run that rely rity. pply y in only illed 3.0 ility, cts). ctor:				
DoS	19-10-2017	6.8	Vuln comp (sub Supp affec Easil allov with prot Succ inter than vuln may addi attac resu inser Java unau subs and part DOS vuln depl runn appl appl	vs una netwo ocols to essful a raction the at erabilit si tional cks of lt in rt or de SE acc uthorize et of Ja unautho ial den) of J erabilit oyment ing san ications	y in of 0 nent: Java 2 loitab uthen rk accord attacked from ttacked y is in gnifica produ- this v unaut elete a essible ed rea ava SE prized ial of ava y ap s, typ dboxe s or hat	the Oracle Dep ions SE: 802 le vu ticated cess via promis s requi a per r and Java S antly ucts. vulnera horized ccess t e data ad acces ability servic SE. N oplies bically ed Java sandbo load	Java Java Java Java Java Java Java Java	ent). are do 9. dility cker tiple SE. man ther the acks pact can data tate, data o a data rtial This Java ents Start Java run	ww e.co hno /se adv cpu 17- 323 htm	36626. nl	JDK 011 192	117/
CV Scoring Scale (C	VSS)	0-1	1-2	2-3	3-4	4-5	5-6		6-7	7-8	8-9	9-10
Vulnerability Type CSRF-Cross Site Rec Injection; XSS- Cros	quest Forgery; Dir	. TravDir	rectory	Traversa	l; DoS-D	enial of	Service;	NA- N	ot Ap	plicable;	Sql-SQ	L

Vulnerability Type(s)	Publish Date	CVSS	Desc	ription & CV	EID	Pat	ch	NCII	PC ID
			comes from on the Java This vulne to Java de servers, the trusted com by an adu Base Scor Integrity an CVSS (CVSS:3.0/2 S:C/C:L/I:L	code (e.g., n the interne a sandbox fo rability does ployments, t at load and de (e.g., code ministrator). e 7.1 (Conf nd Availability AV:N/AC:L/P /A:L). 7 E-2017-103	t) and rely r security not apply ypically ir run only e installec CVSS 3.0 identiality y impacts) Vector R:N/UI:R/	7 7			
NA	19-10-2017	6.8	Vulnerabili SE Embe Oracle Jav RMI). Supp affected a 7u151, 8u Embedded exploitable unauthenti network protocols t Java SE attacks req from a p attacker vulnerabili Embedded, significantl products. S vulnerabili takeover Embedded. vulnerabili deploymen running sa application applets, for untrusted comes from on the Jav	ty in the Jav dded comp a SE (subc orted version are Java SI 144 and 9 8 8u144. vulnerabili cated attac access via o compromis Embedded. uire human erson other and wh ty is in Java SE attacks y impact uccessful atta ty can r of Java SE, Note: ty applies ts, typically ndboxed Java s or sandb	ra SE, Java onent o omponent ns that are E: 6u161 Java SE Easily ty allows ker with multiple se Java SE Successfu interaction than the ile the SE, Java SE additiona acks of this result in Java SE to Java in clients Web Star oxed Java and run code tha t) and rely r security not apply	f ww.o e.com hnetw /secu advis r cpuod s 17- 1 3236 html 1 5 1 5 1 5 1 5 1 5 1 5 1 5 1 5 1 5 1	racl 1/tec vork 1rity- ory/ ct20	A-OR JDK;J 0111 193	-
CV Scoring Scale (C	VSS)	0-1	1-2 2-3	3-4 4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type CSRF-Cross Site Rec Injection; XSS- Cros	(s): quest Forgery; Dir	. TravDir	ectory Travers	al; DoS-Denial of	Service; NA-	Not Appli	cable; S	Gql-SQL	

Vulnerability Type(s)										NCIIP	C ID
JDK;JRE;Jrockit			trus by Base Inte CVS (CVS S:C/	ted coo an adu e Score grity ar	de (e.g ninistra e 9.6 nd Avai AV:N/A I/A:H).	ed 8.0 ty, s). or:					
DoS	19-10-2017	2.6	SE I of C Seri that 6u1 SE R28 vulr una netv prof Java Succ inte thar atta resu caus (par Emh vulr thro app spec usin app spec usin app serv (Ava Vect (CVS	Embedd Dracle Ja alizatio are a 61, 701 Embed 3.15. herabilit uthenti- work tocols t cessful raction h the cks of alt in u se a pa rtial DC bedded, herabilit bugh sau lication lets. It o plying cified ng sand lication lets, su vice. CV ailabilit tor: SS:3.0/A (C:N/I:N	led, JRo ava SE n). Sup affected l51, 8u lded: Difficu ty cated access o comp Embe attacks from attacks from attacks from this v unautho artial d DS) of J JRocl ty can attack artial d DS) of J JRocl ty can attack s and can also data f Comp boxed s or ch as S 3.0 y in AV:N/A V/A:L).	ockit co (subco oported l are 144 ar 8u144; alt to attack via oromise edded, requin a pers ker. S culneral orized lenial co fava SE kit. No be exp co API onent Java V sandbo throug Base npacts) C:H/PF	allow er wi multip Java S JRock re huma son oth Successibility ca ability ca ability ca ability ca bility ca ability ca ability ca bility ca bility ca ability ca bility ca bility ca bility ca ability ca bility ca bility ca ability ca bility ca bility ca ability ca ability ca bility ca ability ca ability ca bility ca ability ca bility	nt wint: e.a ns hr E: /s va ad it: cp oit 17 ws 32 th ht ole E, an er ful an to ce SE nis ed art va by he ut va by he ut va SS	tp://w w.oracl com/tec network security- lvisory/ puoct20 7- 236626. ml	A-OR4 JDK;J- 01111 194	
CV Scoring Scale (C	Oring Scale (CVSS) O-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9							8-9	9-10		

Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS		Desci	ription	& CVE	EID		Patch	NCIIPC ID
NA	19-10-2017	4.3	SE E of O Netv that 6u10 SE R28. vuln unau etw com Emb vuln Emb sign proc vuln unau dele Java acce vuln unau dele Java acce vuln unau dele Java acce vuln unau dele Java acce vuln unau dele Java acce vuln unau dele Java acce vuln unau dele Java acce vuln unau dele Java acce vuln unau dele Java acce vuln unau dele Java acce vuln thro appl appl serv (Inte (CVS S:C/	erability athenticy vork a promise edded, erability edded, ificantly lucts. Su erability athorize te acces SE ssible erability ugh san ications ets. It co olying	ed, JRo va SE va SE). Sup ffected 51, 8u ded: 3 Difficu y ated ccess e Java JRock y is in JRock y is in JRock y can data. y can data. y can data. y can data t Compo coxed s or s ch as SS 3.0 mpacts V:N/A /A:N).	ockit co (subco ported l are 144 an 3u144; attack via l attack via l it, atta bact a date, i ome of edded, Not be date, i ome of edded, Not sandbo be exp co API onent Java V sandbo throug Base 1 5). CVS C:H/PF	ompone mpone versio Java S ad 9; Ja JRock expl allov er w HTTP Java /hile t E, Java Addition cks of tl esult insert f Java S JRocc e: Tl exploit web Sta oxed Ja oloited s in t witho Veb Sta xed Ja ch a w Score 4 S Vecto R:N/UI:	ent ww nt: e.c ns hn SE: /s va ad it: cp oit 17 ws 32 ith ht: to SE he SE ay nal nis in or SE, kit nis ed art va by he out art va by he out art va by he out art va by he out art	36626.	A-ORA- JDK;J- 011117/ 195
DoS	19-10-2017	5	Vuln SE E of O Netv that 6u16 SE R28. vuln	erabilit Imbedd racle Ja vorking are a 51, 7u1 Embed 3.15. erabilit uthentic	y in tl ed, JRo va SE). Sup ffectec 51, 8u ded: 4 Easil y	ent ww nt: e.c ns hn SE: /s va ad cit: cp ole 17	36626.	A-ORA- JDK;J- 011117/ 196		
CV Scoring Scale (CV	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9 9-10	

Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Desc	ription & CVI	EID	Pat	ch	NCIIPC ID
			protocols to Java SE Successful vulnerabilit unauthorize partial den DOS) of Embedded, vulnerabilit through sar applications applets. It o supplying specified using sand applications applets, su service. CV (Availability Vector: (CVSS:3.0/A S:U/C:N/I:N	ty can re ed ability to hial of service Java SE, JRockit. No ty can be ndboxed Java V s and sandbo can also be exj data to API Component boxed Java V s or sandbo ich as throug YS 3.0 Base y impacts)	JRockit. of this esult in cause a e (partial Java SE ote: This exploited Web Start oxed Java ploited by s in the without Web Start oxed Java gh a web Score 5.3 . CVSS R:N/UI:N/			
DoS	19-10-2017	5	Vulnerabilit SE Embedd of Oracle Ja Serialization that are a 6u161, 7u1 SE Embed R28.3.15. vulnerabilit unauthention network protocols to Java SE Successful vulnerabilit unauthorize partial den DOS) of Embedded, vulnerabilit through sar	ty in the Java led, JRockit co ava SE (subco n). Supported affected are 151, 8u144 ar lded: 8u144; Easily e cated attack access via o compromise Embedded, attacks	a SE, Java omponent omponent: l versions Java SE: nd 9; Java JRockit: xploitable allows ker with multiple e Java SE, JRockit. of this esult in cause a e (partial Java SE ote: This exploited Web Start	e.com hnetw /secu: adviso cpuoc 17- 32366 html	racl /tec vork rity- ory/ rt20	A-ORA- JDK;J- 011117/ 197
CV Scoring Scale (C	vss)	0-1	1-2 2-3	3-4 4-5	· · · ·		7-8	8-9 9-10
Vulnerability Type CSRF-Cross Site Rec Injection; XSS- Cros	quest Forgery; Dir	. TravDir	ectory Traversa	ıl; DoS-Denial of S	Service; NA- N	lot Applic	able; S	ql-SQL

Vulnerability Type(s)	Publish Date	CVSS		Descr	iptior	n & CVI	EID		Patch	NCI	IPC ID
			suppl speci using appli apple servic (Avai Vecto (CVSS S:U/O	lying of fied sandt cations ets, suc ce. CVS lability or: S:3.0/A C:N/I:N	data f Compoxed or ch as SS 3.0 v in V:N/A /A:L).	to API onent Java V sandbo throug Base npacts)	R:N/UI:N	he out art va eb 5.3 SS			
Knowledge Ma											
NA	19-10-2017	5.8	Know comp Suite Interf are i 12.1.: and vulne unau netwo comp Mana requi perso while Know may addit attach result critic all Or access unau deleto Know access Score Integ (CVSS	(su face). S affected 3, 12.2. Prability thentic ork a promise gemen re hun or othe the vu yledge sig ional ks of t in un al data cacle Ku sible thorize e acces yledge sible thorize e acces yledge sible thorize e acces yledge sible thorize face (sible thorize (sible (sible (of Or ubcom uppor d are 3, 12.2 7. Eas y ated ccess e Ora t. Such an in r than ulneral Mana gnifica produ this v nautho or co nowled data ed up ss to data. (Cont npacts V:N/A /A:N).	Ma racle E ponent ted ver 12.1.1 2.4, 12.2 sily e attack via 1 acle K ccessfu teractio the att bility is gemen atty acts. S rulneral orized mplete dge Ma as date, f some Ma CVSS fidentia). CVS	nageme -Busine sions th 1, 12.1 2.5, 12.2 xploitab allow ter wi HTTP nowled l attac on from acker an in Orac t, attac bility ca access access nageme well insert of Orac nageme 3.0 Ba allity an S Vecto 2:N/UI:F	ntwesse.hat/s.2,ac.2,ac.2,ac.2,ac.2,ac.2,ac.2,ac.2,ac.2,ac.2,ac.2,ac.2,ac.2,ac.2,ac.2,ac.2,ac.2,ac.1,ac </td <td>ttp://w w.oracl com/tec network security- dvisory/ ouoct20 7- 236626. tml</td> <td></td> <td>RA-)WL- 117/</td>	ttp://w w.oracl com/tec network security- dvisory/ ouoct20 7- 236626. tml		RA-)WL- 117/
CV Scoring Scale (CV	VSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(CSRF-Cross Site Req Injection; XSS- Cross	(s): quest Forgery; Dir	. TravDir	ectory T	[raversa]	l; DoS-D	enial of S	Service; N	A- Not A	Applicable;	Sql-SQL	

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://w ww.oracl e.com/tec hnetwork /security- advisory/ cpuoct20 17- 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://w ww.oracl e.com/tec hnetwork /security- advisory/ cpuoct20 17- 3236626. html	A-ORA- KNOWL- 011117/ 200
CV Scoring Scale (C	VSS)	0-1	1-2 2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10
Vulnerability Type CSRF-Cross Site Rec Injection; XSS- Cros	quest Forgery; Dir	. TravDir	ectory Traversal; DoS-Denial of Service; NA- N	ot Applicable; S	Gql-SQL

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 Se	rvice 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://w ww.oracl e.com/tec hnetwork /security- advisory/ cpuoct20 17- 3236626. html	A-ORA- MOBIL- 011117/ 201
CV Scoring Scale (C	VSS)	0-1	1-2 2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10
Vulnerability Type CSRF-Cross Site Rec Injection; XSS- Cros	quest Forgery; Dir	. TravDir	ectory Traversal; DoS-Denial of Service; NA- N	ot Applicable; S	Gql-SQL

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	T			1	
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://w ww.oracl e.com/tec hnetwork /security- advisory/ cpuoct20 17- 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://w ww.oracl e.com/tec hnetwork /security- advisory/ cpuoct20 17- 3236626. html	A-ORA- MYSQL- 011117/ 203
CV Scoring Scale (C	VSS)	0-1	1-2 2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10
Vulnerability Type CSRF-Cross Site Rec Injection; XSS- Cros	quest Forgery; Dir	. TravDii	ectory Traversal; DoS-Denial of Service; NA- N	lot Applicable; S	ql-SQL

Vulnerability Type(s)	Publish Date	CVSS	D	escription	N & CVE	ID		Patch	NCII	PC ID
			(Availal Vector: (CVSS:3 S:U/C:N	CVSS 3.0 pility in .0/AV:N/A [/I:N/A:H]. : CVE-201	npacts). C:L/PR	. CVS :H/UI:N	SS			
NA	19-10-2017	3.5	Vulnera comport (subcort Support affected 5.7.19 exploit privileg access compro Success vulnera unautho hang o crash (Server. (Availal Vector: (CVSS:3 S:U/C:N	bility in the nent of nponent: S ted versi are 5.6.37 and earli vulnerabil ed attacke via multip mise M ful atta bility ca prized abi or freque complete CVSS 3.0	e MySC Oracle Server: ons t and ea er. Dif ity allo r with ole pro ySQL cks in re lity to ntly ro DOS) c Base S npacts).	QL Serve MySQ InnoDB hat an arlier an fficult t ows hig networ tocols t Serve of th sult i cause epeatab of MySQ Score 4. CVS R:H/UI:N	L www.). e.c. ce hr. d /s co add ch cp k 17 co 32 r. ht is is iz a jL jA jS S	tp://w w.oracl com/tec network ecurity- lvisory/ uoct20 2- 236626. ml	A-OF MYS 0112 204	
NA	19-10-2017	3.5	Vulnera compor (subcor Perform version 5.6.37 a earlier. vulnera attacker multiple MySQL of this unautho hang o crash (Server. (Availal Vector:	bility in the nent of nponent: nance Sche s that an and earlier Difficult bility allow c with net e protocols Server. Su vulnerability or ized abit or freque CVSS 3.0	e MySC Oracle ema). S re affe and 5 t to vs low p work a to cor iccessfu ity con lity to ntly re DOS) c Base S npacts).	QL Serve MySQ Serve upporte cted an explo orivilege ccess vi npromis al attach result i cause epeatabl of MySQ Score 5. CVS	L wy r: e.o d hr re /s d ad it cp d 17 ia 32 se ht ss h t ss f a b c ss f a ss f a b t ss f a b t ss f a b t ss f a b t ss f a b c f s a c f a c f s a c f a c a c	tp://w w.oracl com/tec network ecurity- visory/ uoct20 2 36626. ml	A-OF MYS 0112 205	QL-
CV Scoring Scale (C	VSS)	0-1	1-2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type CSRF-Cross Site Rec Injection; XSS- Cros	quest Forgery; Dir	. TravDir	ectory Tra	versal; DoS-D	enial of S	ervice; NA	- Not A	pplicable; S	ğql-SQL	

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://w ww.oracl e.com/tec hnetwork /security- advisory/ cpuoct20 17- 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://w ww.oracl e.com/tec hnetwork /security- advisory/ cpuoct20 17- 3236626. html	A-ORA- MYSQL- 011117/ 207
NA	19-10-2017	4	Vulnerability in the MySQL Server component of Oracle MySQL	http://w ww.oracl	A-ORA- MYSQL-
CV Scoring Scale (CV		0-1		6-7 7-8	8-9 9-10

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(subcomponent: Server: 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/tec hnetwork /security- advisory/ cpuoct20 17- 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://w ww.oracl e.com/tec hnetwork /security- advisory/ cpuoct20 17- 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://w ww.oracl e.com/tec hnetwork /security- advisory/	A-ORA- MYSQL- 011117/ 210
		0-1	1-2 2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Easily exploitable vulnerabilit allows high privileged attacked with network access via multipl protocols to compromise MySQ Server. Successful attacks of this vulnerability can result i unauthorized ability to cause hang or frequently repeatable crash (complete DOS) of MySQ Server. CVSS 3.0 Base Score 4. (Availability impacts). CVS 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	er 17- e 3236626. L html s n a e L 9 S	
NA	19-10-2017	4	Vulnerability in the MySQL Server component of Oracle MySQ (subcomponent: Grou Replication GCS). Supporte versions that are affected ar 5.7.19 and earlier. Easil exploitable vulnerability allow high privileged attacker wit network access via multipl protocols to compromise MySQ Server. Successful attacks of thi	L ww.oracl p e.com/tec hnetwork e /security- y advisory/ c cpuoct20 h 17- e 3236626. L html s n a e L 9 S	A-ORA- MYSQL- 011117/ 211
NA	19-10-2017	4	Vulnerability in the MySQL Server component of Oracle MySQ (subcomponent: Server: FTS Supported versions that an affected are 5.7.19 and earlie Easily exploitable vulnerabilit allows high privileged attacker with network access via multipl protocols to compromise MySQ Server. Successful attacks of this	L ww.oracl). e.com/tec hnetwork r. /security- y advisory/ er cpuoct20 e 17- L 3236626.	A-ORA- MYSQL- 011117/ 212
CV Scoring Scale (CV		0-1	1-2 2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

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	ww.oracl e.com/tec hnetwork /security- advisory/ cpuoct20 17- 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	ww.oracl e.com/tec hnetwork /security- advisory/ cpuoct20 17- 3236626. html	A-ORA- MYSQL- 011117/ 214
CV Scoring Scale (C	-	0-1	1-2 2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10
Vulnerability Type(CSRF-Cross Site Rec Injection; XSS- Cros	quest Forgery; Dir	. TravDii	ectory Traversal; DoS-Denial of Service; NA-	Not Applicable; S	Sql-SQL

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://w ww.oracl e.com/tec hnetwork /security- advisory/ cpuoct20 17- 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://w ww.oracl e.com/tec hnetwork /security- advisory/ cpuoct20 17- 3236626. html	A-ORA- MYSQL- 011117/ 216
CV Scoring Scale (CV	VSS)	0-1	1-2 2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10
Vulnerability Type CSRF-Cross Site Rec Injection; XSS- Cros	quest Forgery; Dir	. TravDir	ectory Traversal; DoS-Denial of Service; NA- N	ot Applicable; S	ql-SQL

Type(s) Date NA 19-10-2017 NA 19-10-2017 NA 19-10-2017				NCIIPC ID
		CVE ID : CVE-2017-10227		
NA 19-10-2017		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://w ww.oracl e.com/tec hnetwork /security- advisory/ cpuoct20 17- 3236626. html	A-ORA- MYSQL- 011117/ 217
	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://w ww.oracl e.com/tec hnetwork /security- advisory/ cpuoct20 17- 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://w ww.oracl e.com/tec hnetwork	A-ORA- MYSQL- 011117/ 219
CV Scoring Scale (CVSS)	0-1	1-2 2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

CSRF-Cross Site Request Forgery; Dir. Trav.-Directory 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 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/ cpuoct20 17- 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://w ww.oracl e.com/tec hnetwork /security- advisory/ cpuoct20 17- 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://w ww.oracl e.com/tec hnetwork /security- advisory/ cpuoct20 17-	A-ORA- MYSQL- 011117/ 221
CV Scoring Scale (CV Vulnerability Type(CSRF-Cross Site Rec Injection; XSS- Cros	(s): quest Forgery; Dir	0-1 . TravDir	1-2 2-3 3-4 4-5 5-6 ectory Traversal; DoS-Denial of Service; NA- N	6-7 7-8 ot Applicable; S	8-9 9-10 ql-SQL

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 Connecto					
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://w ww.oracl e.com/tec hnetwork /security- advisory/ cpuoct20 17- 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://w ww.oracl e.com/tec hnetwork /security- advisory/ cpuoct20 17- 3236626. html	A-ORA- MYSQL- 011117/ 223
CV Scoring Scale (C	VSS)	0-1	1-2 2-3 3-4 4-5 5-6 0	6-7 7-8	8-9 9-10
Vulnerability Type((s): quest Forgery; Dir	. TravDiı	rectory Traversal; DoS-Denial of Service; NA- N	ot Applicable; S	ql-SQL

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 Enterpri					[
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://w ww.oracl e.com/tec hnetwork /security- advisory/ cpuoct20 17- 3236626. html	A-ORA- MYSQL- 011117/ 224
Outside In Tecl	hnology				
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://w ww.oracl e.com/tec hnetwork /security-	A-ORA- OUTSI- 011117/ 225
CV Scoring Scale (C	VSS)	0-1	1-2 2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10
Vulnerability Type	(s): quest Forgery; Dir	. TravDir	rectory Traversal; DoS-Denial of Service; NA- N	ot Applicable; S	ql-SQL

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).	advisory/ cpuoct20 17- 3236626. html	
		<i></i>	CVE ID : CVE-2017-10051		
Peoplesoft Enter Gain Information	erprise Fin Sta 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://w ww.oracl e.com/tec hnetwork /security- advisory/ cpuoct20 17- 3236626. html	A-ORA- PEOPL- 011117/ 226
CV Scoring Scale (CV	VSS)	0-1	1-2 2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10
Vulnerability Type CSRF-Cross Site Rec Injection; XSS- Cros	quest Forgery; Dir	. TravDir	ectory Traversal; DoS-Denial of Service; NA- N	ot Applicable; S	ql-SQL

Vulnerability Type(s)	Publish Date	CVSS	Desc	riptior	1 & CVE	ID		Patch	NCIIF	'C ID
		e Carrii	(Confident Vector: (CVSS:3.0/ S:U/C:L/I:N CVE ID : CV	AV:N/A I/A:N). / E-201	AC:L/PR 7-1016	:L/UI:N, <u>4</u>	/			
Peoplesoft Ente										Δ
NA	19-10-2017	4.9	(subcompo supported is 9.2. vulnerabili attacker w HTTP to o Enterprise require hu person otl Successful vulnerabili unauthoriz delete ac PeopleSoft accessible unauthoriz subset of HCM acce Base Score Integrity i (CVSS:3.0/ S:U/C:L/I:I CVE ID : CV	HCM Peoples ment: versior Easil ty allov ith net compro HCM. S man in her tha atta ty ca ed up ccess Ent data ed rea People ssible 4.6 (Co mpacts AV:N/A A/A:N). /E-201	compo Soft Securit in that is ly ex- vs low p work a mise P- uccessfi teractio an the cks of an re- date, if to so terprise as - ad acce eSoft E data. (onfident c:L/PR 7-1030	onent of Product Product y). The affecte ploitable orivilege ccess vi- eopleSo al attack n from attacke of the sult i nsert of HCl well a ess to nterpris CVSS 3. iality an S Vecto :L/UI:R, 6	of ww ts e.c. he hm d /s le ad d cp ia 17 ft 32 ts ht a r. ft 32 ts ht a r. of M s a e 0 d r: /	236626. ml	A-OR. PEOP 0111 227	°L- 17/
NA	19-10-2017	4.9	Vulnerabili Enterprise Oracle (subcompo supported is 9.2. vulnerabili attacker w HTTP to o Enterprise require hu person oth while the PeopleSoft	HCM Peoples onent: versior Easil ty allow ith net compro HCM. S man in er than	compo Soft Securit that is ly ex vs low p work a mise P uccessfu teractio the atta	onent of Product y). Th affecte ploitabl orivilege ccess vi eopleSo ul attack n from acker an	of ww ts e.c. d /s d /s le ad d cp ia 17 ft 32 ts ht a d n	tp://w w.oracl com/tec network ecurity- lvisory/ uoct20 2- 236626. ml	A-OR PEOP 0111 228	'L-
CV Scoring Scale (CV	VSS)	0-1	1-2 2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(CSRF-Cross Site Rec Injection; XSS- Cros	quest Forgery; Dir	. TravDir	ectory Travers	al; DoS-D	enial of S	ervice; NA	- Not Aj	pplicable; S	Sql-SQL	

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE IDPatchNCIIPC 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 							
Peoplesoft Ente										
Gain Information	19-10-2017	2.1	Vulnerability in the PeopleSofthttp://wA-ORA-EnterprisePTPeopleToolsww.oraclPEOPL-component of Oracle PeopleSofte.com/tec011117/Products(subcomponent:hnetwork229Application Server).Supported/security-versions that are affected are 8.54,advisory/2298.55 and 8.56.Easily exploitablecpuoct20vulnerabilityallows17-unauthenticatedattacker with3236626.logon to the infrastructure wherehtmlPeopleSoftEnterprisePTPeopleToolsExecuteutestocompromise PeopleSoft EnterprisePTPT PeopleTools.Successful attacksof this vulnerability can result inunauthorized access to criticaldata or complete access to allPeopleSoftPeopleTools accessible data.CVSS3.0 Base Score 6.2 (Confidentialityimpacts).CVSSVector:(CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).CVE ID : CVE-2017-10351							
Gain Information	19-10-2017	4.3	Vulnerability in the PeopleSofthttp://wA-ORA-EnterprisePeopleToolsww.oraclPEOPL-component of Oracle PeopleSofte.com/tec011117/Products (subcomponent: Updateshnetwork230Change Assistant). The supported/security-version that is affected is 8.54.advisory/							
CV Scoring Scale (C	VSS)	0-1	1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10							
CSRF-Cross Site Rec	CV Scoring Scale (CVSS) Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. TravDirectory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;									

NA 19-10-2017 4.3 Vulnerability cares via use to the vulnerability cares via use to critical data crossible data. CVSS 3.0 Base Score 5.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/A:V)/AC:H/PR:N/UI:N/S:U/C:H/I:N/S:U/C:S/S:A:A A-ORA-P:OPIESONT	Vulnerability Type(s)	Publish Date	CVSS	Description & CVE IDPatchNCIIPC ID
NA 19-10-2017 4.3 Vulnerability in the PeopleSoft Enterprise http://w 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 http://w advisory/ geucrity A-ORA- PEOPL- 011117/ NA 9.55 and 8.56. Easily exploitable vulnerability geucrity- advisory/ allows yeucrity- geucrity NA 9.55 and 8.56. Easily exploitable vulnerability geucrity- advisory/ allows geucrity- geucrity NA 9.65 and 8.56. Easily exploitable vulnerability allows 17- 3236626. NH 9.70-2017 17- 3236626. NH 9.70-2017 17- 3236626. NH 9.70-2017 17- 3236626. NH 9.20-2017 11.17/ 3236626. NH 9.20-2017-10382 11.127 NH 9.20-2017 12.22 24.1 <td></td> <td></td> <td></td> <td>allows unauthenticated attacker 17- with network access via HTTP to 3236626. compromise PeopleSoft Enterprise html 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).</td>				allows unauthenticated attacker 17- with network access via HTTP to 3236626. compromise PeopleSoft Enterprise html 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).
Gain Information19-10-20175Vulnerability Enterpriseinthe PTPeopleSoft PeopleToolshttp://w Ww.oraclA-ORA- PEOPL-0.11.22.33.44.55.66.77.88.99.10	NA	19-10-2017	4.3	Vulnerability in the PeopleSofthttp://wA-ORA-EnterprisePeopleToolsww.oraclPEOPL-component of Oracle PeopleSofte.com/tec011117/Products (subcomponent: PIAhnetwork231CoreTechnology). Supported/security-versions that are affected are 8.54,advisory/8.55 and 8.56. Easily exploitablecpuoct20vulnerabilityallows17-unauthenticatedattacker withnetworkaccess viaPeopleTools.Successfulattacksrequire human interaction from aperson other than the attacker andwhilethe vulnerability is inPeopleSoftEnterprisePeopleTools,attacksvulnerability ican result inunauthorized update, insert ordeleteaccess to some ofPeopleSoft Enterprise PeopleToolsaccessibledata.CVSS 3.0 AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:L/A:N).
		19-10-2017	5	Vulnerability in the PeopleSoft http://w A-ORA-
	CV Scoring Scale (C	V(SC)	0-1	

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			component of Oracle 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/tec hnetwork /security- advisory/ cpuoct20 17- 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://w ww.oracl e.com/tec hnetwork /security- advisory/ cpuoct20 17- 3236626. html	A-ORA- PEOPL- 011117/ 233
Gain Information	19-10-2017	5	Vulnerability in the PeopleSoftEnterprisePeopleToolscomponent of Oracle PeopleSoftProducts (subcomponent: TestFramework).Supported versionsthat are affected are 8.54, 8.55 and	http://w ww.oracl e.com/tec hnetwork /security- advisory/	A-ORA- PEOPL- 011117/ 234
CV Scoring Scale (C	_	0-1	1-2 2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10
Vulnerability Type CSRF-Cross Site Rec Injection; XSS- Cros	quest Forgery; Dir	. TravDir	ectory Traversal; DoS-Denial of Service; NA- N	ot Applicable; S	ql-SQL

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).		
NA	19-10-2017	5.5	CVE ID : CVE-2017-10280Vulnerability in the PeopleSoftEnterprisePTPeopleToolscomponent of Oracle PeopleSoftProducts(subcomponent:PeopleSoft CDA). The supportedversion that is affected is 8.56.Easily exploitable vulnerabilityallows low privileged attackerwith network access via HTTP tocompromise PeopleSoft EnterprisePTPeopleTools. While thevulnerability is in PeopleSoftEnterprise PT PeopleTools, attacksmaysignificantlyadditionalproducts. Successfulattacks of this vulnerability canresult in unauthorized update,insert or delete access to some ofPeopleSoftEnterprisePTPeopleToolsaccessibledata.CVSS 3.0BaseScore6.4(Confidentiality andIntegrity impacts).CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:N).CVE ID : CVE-2017-10418		A-ORA- PEOPL- 011117/ 235
DoS	19-10-2017	5.5	VulnerabilityinthePeopleSoftEnterprisePeopleTools		A-ORA- PEOPL-
		0-1	1-2 2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

CSRF-Cross Site Request Forgery; Dir. Trav.-Directory 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 NCI	IIPC ID									
			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 	1117/									
NA	19-10-2017	5.5	Enterprise PeopleTools ww.oracl PEO	DRA- DPL- 1117/ 7									
CV Scoring Scale (C	VSS)	0-1	1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9	9-10									
CSRF-Cross Site Req	quest Forgery; Dir	. TravDir	irectory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQ	CV Scoring Scale (CVSS) Image: CV Scoring Scale (CVSS) Image: CV Scoring Scale (CVSS) Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. TravDirectory 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
	Date		S:U/C:H/I:H/A:N). CVE ID : CVE-2017-10364		
NA	19-10-2017	5.8	Vulnerability in the PeopleSoftEnterprisePeopleToolscomponent of Oracle PeopleSoftProducts (subcomponent: PIACoreTechnology). Supportedversions that are affected are 8.54,8.55 and 8.56. Easily exploitablevulnerabilityallowsunauthenticatedattacker withnetworkaccess via HTTP tocompromise PeopleSoft EnterprisePeopleTools.Successful attacksrequire human interaction from aperson other than the attacker andwhile the vulnerability is inPeopleSoftEnterprisePeopleTools,attacksattacksmaysignificantlyimpactadditionalproducts.Successful attacks of thisvulnerabilitycanresultinunauthorizedupdate, insert ordeleteaccessaccessibledataas wellasunauthorizedreadaccess toasubset of PeopleSoftEnterprisePeopleTools accessibledata. CVSS3.0 BaseScore 6.1 (ConfidentialityandIntegrityandIntegrityimpacts).CVSSVector:(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://w ww.oracl e.com/tec hnetwork /security- advisory/ cpuoct20 17- 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://w ww.oracl e.com/tec hnetwork /security- advisory/ cpuoct20 17- 3236626. html	A-ORA- PEOPL- 011117/ 239
CV Scoring Scale (C	_	0-1	1-2 2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10
Vulnerability Type CSRF-Cross Site Rec Injection; XSS- Cros	quest Forgery; Dir	. TravDii	rectory Traversal; DoS-Denial of Service; NA- N	ot Applicable; S	ql-SQL

Type(s)	Date											
NA	19-10-2017	5.8	requipers whill Peop sign procevuln unat dele Peop accee unat subs Peop 3.0 1 and Vect (CVS S:C/ CVE Vuln Ente com Proce Supp affee Easi allow with com Peop sign procevuln unat dele Peop 3.0 1 and Vect (CVS S:C/ CVE Ente com Proce Supp affee Easi allow with com Peop acceeul acceul vuln Proce Supp affee Easi allow with com Peop sign Peop acceul supp affee Easi allow vuln Peop requipers vuln Peop acceul sign Peop acceul acceul vuln Proce Supp affee Easi allow vuln Peop requipers vuln Peop requipers vuln Peop sign Peop acceul acceul sign Peop acceul sign Peop acceul acceul supp affee Peop acceul supp affee Peop acceul supp affee Peop acceul sign Peop acceul sign Peop acceul sign Peop acceul sign Peop acceul sign Peop affee Peop acceul sign Peop acceul sign Peop acceul sign Peop acceul sign Peop acceul sign Peop acceul sign Peop acceul sign Peop acceul sign Peop acceul sign Peop acceul sign Peop acceul sign Peop acceul sign Peop acceul sign Peop acceul sign acceul si acceul si ac acceul sign acceul	pleSoft essible uthorize set of pleTool Base Sc Integ cor: SS:3.0/A C:L/I:L ID:CV herabilit erprise ponent ducts (s ported cted ar ly exp ws una netwo promis pleTool aire hun son othe le the pleSoft pleTool ificantly ducts. Si herabilit uthorize te ac pleSoft essible	nan in er than vuln s, y imp uccess ed up cess Enterp data ed rea People s acces ore 6.1 rity in V:N/A (A:N). E-201 ty in of Or subcom versi e 8.54, oloitabl authen ork acce e Peop s. Suc man in er than vuln s, y imp uccess Enterp data	teracti the att erabili attacks pact ful atta an r date, to s rise Pe as ad acc esoft ful atta as cesoft ful atta cess ful ticated ess via le vu ticated ess via le vu ticated ess via le soft ful attacks pact ful atta an r date, to s rise Pe as as as as as cessfu ticated ess via le vu ticated ess via le vu ticated ess via le cessfu ticated ess ful attacks pact ful atta	on from tacker a ty is Enterpresent additio cks of t esult insert some eopleTo well esss to Enterpresent atta. CV idential s). CV R:N/UI: B1 PeopleS eopleTo PeopleS eopleTo PeopleS t: Quent that a and 8. Inerabil attach a HTTP Enterpresent that a to from tacker a ty is Enterpresent additio cks of t esult insert some eopleTo	n a and in rise hay hal his of ols a rise //SS lity //SS R/ fools for soft of the second in rise hay hal his in of ols as a rise //SS are //SS hard fools for y).	ww e.co hne /sec adv cpu 17-	o://w .oracl om/tec twork curity- isory/ oct20 :6626. il	PEC	PRA- DPL- 117/
		0-1	una 1-2	uthorize	ed rea	ad acc	ess to		-7	7-8	8-9	9-10
CV Scoring Scale (C Vulnerability Type	-											

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).
NA	19-10-2017	5.8	Vulnerability in the PeopleSofthttp://wA-ORA-EnterprisePeopleToolsww.oraclPEOPL-component of Oracle PeopleSofte.com/tec011117/Products (subcomponent: Core).hnetwork241Supported versions that are/security-affected are 8.54, 8.55 and 8.56.advisory/Easily exploitable vulnerabilitycpuoct20allows unauthenticated attacker17-with network access via HTTP to3236626.compromise PeopleSoft EnterprisehtmlPeopleTools.Successful attacksrequire human interaction from aperson other than the attacker andwhile the vulnerability is inPeopleSoftPeopleSoftEnterprisePeopleTools, attacks maysignificantly impact additionalproducts.Successful attacks of thisvulnerability can result inunauthorized update, insert ordelete access to some ofPeopleSoft EnterprisePeopleTools accessible data as well assunauthorized read access to asubset of PeopleSoft EnterprisePeopleTools accessible data. CVSS3.0 Base Score 6.1 (Confidentialityand Integrity impacts).CVSSVector:(CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).CVE ID : CVE-2017-10158
DoS	19-10-2017	6.4	Vulnerability in the PeopleSofthttp://wA-ORA-EnterprisePeopleToolsww.oraclPEOPL-component of Oracle PeopleSofte.com/tec011117/Products(subcomponent:hnetwork242Sawbridge).Supported versions/security-that are affected are 8.54, 8.55 andadvisory/
CV Scoring Scale (C	-	0-1	1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10
Vulnerability Type CSRF-Cross Site Rec Injection; XSS- Cros	quest Forgery; Dir	. TravDir	rectory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL

Vulnerability	Publish Date	CVSS	Description & CVE ID Patch NCI	IPC ID
Type(s)	Date		8.56.Easilyexploitablecpuoct20vulnerabilityallows17-unauthenticatedattackerwithnetworkaccessviaHTTPtohtmlcompromise PeopleSoft EnterprisehtmlPeopleTools.Whilethevulnerabilityisin PeopleSoftEnterprisePeopleTools, attacksmaysignificantlyimpactadditionalproducts.Successfulattacks of this vulnerability canresult in unauthorized read accesstoasubsetofPeopleSoftEnterprisePeopleTools accessibledataandunauthorized ability tocause a partial denial of service(partialDOS)ofPeopleSoftEnterprisePeopleTools.CVSS3.0BaseScore 7.2 (Confidentiality andAvailability 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	
NA	19-10-2017	7.5	Vulnerability in the PeopleSofthttp://wA-OEnterprisePTPeopleToolsww.oraclPEO	
Peoplesoft Ente			on Hub	
NA	19-10-2017	5.8 0-1	Vulnerability in the PeopleSofthttp://wA-O1-22-33-44-55-66-77-88-9	RA- 9-10
	(s): quest Forgery; Dir		rectory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL	
Injection; XSS- Cros	s Site Scripting;			

Vulnerability Type(s)	Publish Date	CVSS	Des	cription & CVI	E ID	Pa	tch	NCII	PC ID
			componen Products Enterprise version th Easily ex allows un with netw compromis PRTL Inte attacks rea from a p attacker vulnerabili Enterprise attacks m additional attacks of result in critical dat all People Interaction well as insert or of PeopleSoft Interaction CVSS 3.0 (Confident impacts). (CVSS:3.0/	Portal). The s at is affected ploitable vul authenticated ork access via se PeopleSoft F raction Hub. S quire human in erson other and whi ty is in F PRTL Interact ay significant products. S this vulneral unauthorized soft Enterprise Hub accessio unauthorized lelete access to Enterprise Hub accessio Unauthorized lelete access to Enterprise Hub accessio Unauthorized lelete access to Enterprise Allow accessio Constant CVSS AV:N/AC:L/PF	PeopleSoft omponent: supported is 9.1.00. Inerability attacker a HTTP to Enterprise Successful nteraction than the ele the PeopleSoft ction Hub, ly impact Successful bility can access to access to ise PRTL le data as update, o some of e PRTL ible data. core 8.2 Integrity Vector: R:N/UI:R/	e.con hnet /sec advis cpuc 17- 3236 html	n/tec work urity- sory/ oct20	PEO 0111 244	
NA	19-10-2017	5.8	Enterprise componen Products Enterprise version th Easily ex allows ur with netw compromis PRTL Inte attacks rec	ity in the F PRTL Interact t of Oracle F (subco Portal). The s at is affected ploitable vul authenticated ork access via se PeopleSoft F raction Hub. S quire human in erson other and whi	ction Hub PeopleSoft omponent: supported is 9.1.00. Inerability attacker that HTTP to Enterprise Successful nteraction than the	ww.e e.con hnet /sec advis cpuc 17- 3236 html	oracl n/tec work urity- sory/ oct20	A-OF PEO 0111 245	PL-
CV Scoring Scale (C	-	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. TravDirectory 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 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 Ente	prnrise Scm Fi	nrocure			
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://w ww.oracl e.com/tec hnetwork /security- advisory/ cpuoct20 17- 3236626. html	A-ORA- PEOPL- 011117/ 246

Vulnerability Type(s)	Publish Date	CVSS	J	Descriptio	n & CVE	ID		Patch	NCIIP	C ID
			accessi Score Integri (CVSS: S:C/C:I	orise SCM ible data. 6.1 (Con ity impacts 3.0/AV:N/A L/I:L/A:N). D:CVE-201	CVSS nfidentia s). CVSS AC:L/PR	llity an S Vector .:N/UI:R,	e d r:			
Peoplesoft Ente	erprise Scm St	trategic	Sourcin	ıg						
Gain Information	19-10-2017	5	Enterp Oracle (subco Sourcin that i exploit low j netwon compre FSCM. vulnera unauth subset FSCM Base impact (CVSS: S:U/C:J	imponent: ng). The su s affected table vuln privileged rk access omise Peop Successful ability c norized re of Peopl accessible Score 4.3	A comp eSoft upported i is 9.2 nerability attack via H pleSoft E l attack can re ad acce leSoft E data. (Confi VSS AC:L/PR	onent of Product Strategi d versio 2. Easil y allow er wit HTTP t Interpris s of thi esult i ess to Interpris CVSS 3. dentialit Vector :L/UI:N/	of ww ss e.c. ic hm n /s y ad rs cp h 17 so 32 se ht is n a e 0 y r:	tp://w w.oracl com/tec network ecurity- lvisory/ ouoct20 7- 236626. ml	A-ORA PEOP 01111 247	L-
Peoplesoft Ente	erprise Staffir	a Front			17-1020	1			1	
NA	19-10-2017	4	Vulner Enterp Oracle (subco Office) is affec vulnera privile access People Succes vulnera unauth subset FSCM	mponent: . The support cted is 9.2. I ability ged attack via HTTP Soft Ent sful atta ability c norized re of Peopl accessible Score 2.7 ts). C	A comp eSoft Staffin orted ver Easily es allows er with terprise acks an re acks can re ad acce leSoft E data. (Confi VSS	onent of Product g Fron rsion that ploitabl hig networ npromis FSCM of thi ess to Interpris CVSS 3. dentialit Vector	of ww ss e.c. ht hn at /s le ad h cp k 17 se 32 1. ht is n a se 0 y r:	236626. ml	A-ORA PEOP 01111 248	L-
CV Scoring Scale (C	VSS)	0-1	1-2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type CSRF-Cross Site Rec Injection; XSS- Cros	quest Forgery; Dir	. TravDir	ectory Tra	aversal; DoS-I	Denial of S	ervice; NA	- Not Aj	pplicable; S	Sql-SQL	

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 Off	ĩce						
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://w ww.oracl e.com/tec hnetwork /security- advisory/ cpuoct20 17- 3236626. html	A-ORA- RETAI- 011117/ 249		
Retail Point-of-			CVE ID : CVE-2017-10423				
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://w ww.oracl e.com/tec hnetwork /security- advisory/ cpuoct20 17- 3236626. html	A-ORA- RETAI- 011117/ 250		
CV Scoring Scale (CV	VSS)	0-1	1-2 2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10		
CSRF-Cross Site Req	Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. TravDirectory 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 II					
			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 P	oint Of Service	e.	CVE ID : CVE-2017-10005					
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, advisory/ 7.1.6 and 15.0.1. Difficult to exploit cpuoct20 vulnerability unauthenticated attacker with attacker with access via HTTP to compromise 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 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 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 Accessible data And unauthorized ability to cause a partial denial of service (partial DOS) 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 Accessible data And unauthorized Accessible					
CV Scoring Scale (C	VSS)	0-1	1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-1					
CSRF-Cross Site Rec	/ulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. TravDirectory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL njection; XSS- Cross Site Scripting;							

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID F	Patch	NCIIPC ID			
	Date		(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 Servic	e;Security Ser	vice Fm	W	·				
NA	19-10-2017	4.3	VulnerabilityintheOraclehttpSecurityServicecomponentofwwwOracleFusionMiddlewaree.co(subcomponent:C Oracle SSL API).hndSupportedversionsthatareaffectedareFMW:11.1.1.9.0and12.1.3.0.0.Difficulttoexploitvulnerabilityallows17-	v.oracl om/tec etwork ecurity- visory/ uoct20 - 36626.	A-ORA- SECUR- 011117/ 252			
Siebel Core-ser			Vulnorability in the Siebel Core btt	m. / /				
NA	19-10-2017		Oracle Siebel CRM e.cd (subcomponent: Services). hnd Supported versions that are /se affected are 16.0 and 17.0. Easily adv exploitable vulnerability allows cpu low privileged attacker with 17- network access via HTTP to 323 compromise Siebel Core - Server htm 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	v.oracl om/tec etwork ecurity- visory/ uoct20 - 36626. nl	A-ORA- SIEBE- 011117/ 253			
CV Scoring Scale (CV	VSS)	0-1	1-2 2-3 3-4 4-5 5-6 6-7	7-8	8-9 9-10			
CSRF-Cross Site Req	/v Scoring Scale (CVSS) /ulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. TravDirectory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL njection; XSS- Cross Site Scripting;							

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 Custome	er Relationshi	n Manad	gement 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	/security- advisory/	A-ORA- SIEBE- 011117/ 254
Siebel Ui Frame		_		1 //	4.004
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://w ww.oracl e.com/tec hnetwork /security- advisory/ cpuoct20 17- 3236626. html	A-ORA- SIEBE- 011117/ 255 8-9 9-10
CV Scoring Scale (CV	VSS)	0-1	1-2 2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10
Vulnerability Type(CSRF-Cross Site Rec Injection; XSS- Cros	quest Forgery; Dir	. TravDir	ectory Traversal; DoS-Denial of Service; NA- N	ot Applicable; S	ql-SQL

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. /security- Easily exploitable vulnerability allows unauthenticated attacker cpuoct20 with network access via HTTP to compromise Siebel UI Framework. Successful attacks require human interaction from a person other 				
NA	19-10-2017	5.8	Vulnerability in the Siebel UIhttp://wA-ORA-Framework component of Oracleww.oraclSIEBE-Siebel CRM (subcomponent: UIFe.com/tec011117/Open UI). Supported versions thathnetwork257are affected are 16.0 and 17.0./security-Easily exploitablevulnerabilityadvisory/allowsunauthenticatedattackercpuoct20with network access via HTTP to17-compromise Siebel UI Framework.3236626.Successful attacks require humanhtmlinteraction from a person otherhtmlthan the attacker and while thevulnerability is in Siebel UIFramework,attacksmaysignificantlyimpactadditional				
CV Scoring Scale (C	VSS)	0-1	1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10				
	quest Forgery; Dir	. TravDir	rectory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL				
Injection; XSS- Cross Site Scripting;							

Type(s)			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:	
	19-10-2017	5.8	Framework component of Oracle ww.oracl Siebel CRM (subcomponent: UIF e.com/tec	A-ORA- SIEBE- 011117/ 258
DoS	19-10-2017	6.5	Framework component of Oracle ww.oracl Siebel CRM (subcomponent: EAI). e.com/tec	A-ORA- SIEBE- 011117/ 259
CV Scoring Scale (CVS	SS)	0-1	1-2 2-3 3-4 4-5 5-6 6-7 7-8	8-9 9-10

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/ cpuoct20 17- 3236626. html			
Soa Suite			CVE ID : CVE-2017-10333				
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://w ww.oracl e.com/tec hnetwork /security- advisory/ cpuoct20 17- 3236626. html	A-ORA- SOA S- 011117/ 260		
CV Scoring Scale (C	VSS)	0-1	1-2 2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10		
CSRF-Cross Site Rec	CV Scoring Scale (CVSS) Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. TravDirectory 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
Solaris Cluster			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		
DoS	19-10-2017	4.4	Vulnerability in the Solaris Cluster component of Oracle Sun Systems	http://w ww.oracl	A-ORA- SOLAR-
			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).	e.com/tec hnetwork /security- advisory/ cpuoct20 17- 3236626. html	011117/261
Sparc-sun Syst	em Firmware		CVE ID : CVE-2017-3588		
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://w ww.oracl e.com/tec hnetwork	A-ORA- SPARC- 011117/ 262
CV Scoring Scale (C	VSS)	0-1	1-2 2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10
Vulnerability Type CSRF-Cross Site Rec Injection; XSS- Cros	uest Forgery; Dir	. TravDir	ectory Traversal; DoS-Denial of Service; NA- N	ot Applicable; S	ql-SQL

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID Patch No	CIIPC ID				
			supported version that is affected /security- is Prior to 9.7.6.b. Easily advisory/ exploitable vulnerability allows cpuoct20 high privileged attacker with logon 17- to the infrastructure where SPARC 3236626. M7, T7, S7 based Servers html 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					
Trade Manage	ment							
NA	19-10-2017	5.8	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, advisory/ 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 accessibleTH e.com/tec 01 hnetwork 26 (security- advisory/ 17- 3236626. html	ORA- RADE- 11117/ 53				
CV Scoring Scale (CV	VSS)	0-1	1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-	9 9-10				
CSRF-Cross Site Req	Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. TravDirectory 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://w ww.oracl e.com/tec hnetwork /security- advisory/ cpuoct20 17- 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://w ww.oracl e.com/tec hnetwork /security- advisory/ cpuoct20 17-	A-ORA- TRADE- 011117/ 265
CV Scoring Scale (CV		0-1	1-2 2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Vulnerability	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Type(s)	Date		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:	3236626. html	
Universal Wey	k Quana		(CVSS:3.0/AV:N/AC:L/PR:N/UI:R/ S:C/C:H/I:L/A:N). CVE ID : CVE-2017-3444		
Universal Work	19-10-2017	5	VulnerabilityintheOracleUniversal Work Queue componentofOracleE-BusinessSuite(subcomponent:Administration).Supportedversionsthatareaffected are12.1.1,12.1.2,12.1.3,12.2.3,12.2.4,12.2.5,12.2.6and12.2.7.EasilyexploitablevulnerabilityallowsunauthenticatedattackerwithnetworkaccessviaHTTPtocompromiseOracleUniversalWork Queue.Successful attacks ofthisunauthorizedaccesstocriticaldataorcompleteaccesstoOracleUniversalWorkQueueaccessibledata.CVSS3.0BaseScore7.5(Confidentialityimpacts).CVSSVector:(CVSS:3.0/AV:N/AC:L/PR:N/UI:N/	http://w ww.oracl e.com/tec hnetwork /security- advisory/ cpuoct20 17- 3236626. html	A-ORA- UNIVE- 011117/ 266
CV Scoring Scale (C	-	0-1	1-2 2-3 3-4 4-5 5-6	b-7 7-8	8-9 9-10
Vulnerability Type CSRF-Cross Site Rec Injection; XSS- Cros	quest Forgery; Dir	. TravDir	ectory Traversal; DoS-Denial of Service; NA- N	ot Applicable; S	ql-SQL

Vulnerability	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Type(s)	Date		S:U/C:H/I:N/A:N).		
Virtual Directo			CVE ID : CVE-2017-10332		
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 Vectors (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/ S:U/C:H/I:H/A:H). CVE ID : CVE-2017-10369	ww.oracl e.com/tec hnetwork /security- advisory/ cpuoct20 17- 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	ww.oracl e.com/tec hnetwork /security- advisory/ cpuoct20 17- 3236626. html	A-ORA-VM VI- 011117/ 268
CV Scoring Scale (CV	VSS)	0-1	1-2 2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10
Vulnerability Type(CSRF-Cross Site Req Injection; XSS- Cros	uest Forgery; Dir	. TravDir	ectory Traversal; DoS-Denial of Service; NA-	Not Applicable; S	Gql-SQL

Vulnerability Type(s)	Publish Date	CVSS		Desc	riptior	1 & CVE	ID		Patch	NCIIPC ID
		4.2	Virt 5.0 Avai (CVS S:C/ CVE	ualBox. (Confid lability SS:3.0/ <i>F</i> C:L/I:L, ID : CV	CVSS entiali impac AV:L/A /A:L). <u>E-201</u>	OS) of C 3.0 Ba ty, Integ ts). CVS C:H/PR 7-1042	se Sco grity a S Vecto :H/UI:N 8	ore nd or: N/		
NA	19-10-2017	4.3	Virtu Virtu Core is af expl high to th VM com Virtu is in may addi atta- resu caus repe of O unau dele Virtu unau subs acce Scor Inte CVS (CVS	ualBox ualization fected i oitable privile ne infra virtua promis ualBox. Oracle tional cks of lt in u se a eatable racle VI uthorize te acces ualBox uthorize set of ssible re 7 grity an SS:3.0/ <i>H</i> C:L/I:L, ID : CV	component supponent supponent supponent supponent component ged att structur lBox e While VM Vi gnifica produ this v nauthor hang crash M Virtur ed up ss to so access ed rea Oracle data. 7.3 d Avai AV:L/A (A:H). E-201	acts. S vulnerat orized a or fi (compl ualBox a date, i ome of C sible c ad acce VM V CVSS 5 (Confic lability C:L/PR: 7-1040	of Orac mponents sion the 30. Eas vallow reith log re Orac eutes vallow re orac vallow re orac vallow re orac eutes vallow re orac orac eutes vallow re orac eutes vallow re orac orac eutes vallow re orac orac eutes vallow re orac orac orac orac orac orac orac orac	cle wy nt: e.c. nat hr ily /s ws ad on cp cle 17 to 32 YM ht ity ks at ful an to y S) as or YM nd a ox se ty, s). or: I/	236626. ml	A-ORA-VM VI- 011117/ 269
NA	19-10-2017	4.3	Virt Virt Core is af expl high	ualBox ualization e). The fected i oitable privile	compo on suppor s Prior vulno ged att	the Or onent of (subcon- rted ver to 5.1.3 erability cacker w ure whe	of Orac mponen rsion th 30. Eas 7 allow rith log	cle wy nt: e.c nat hr ily /s ws ad on cp	tp://w w.oracl com/tec tetwork ecurity- lvisory/ uoct20 2-	A-ORA-VM VI- 011117/ 270
CV Scoring Scale (CV	/SS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9 9-10

Vulnerability Type(s)	Publish Date	CVSS		Descr	iption	ı & CVI	EID		Patch	NCI	IPC ID
			comj Virtu is in may addit attac resul caus repe of Or unau delet Virtu unau subs acces Score Integ CVSS (CVS	tional ks of t in un e a atable of racle VM thorize te acces nalBox nthorize et of (ssible of e 7. grity and	While VM Vi gnifica produ this v nautho hang crash 1 Virtu d up s to so access d rea Dracle data. 3 d Avai V:L/A	Oracle the vul rtualBo ntly icts. S ulneral orized or f (comp ialBox date, date, sible date, VM V CVSS (Confi lability	v nerabili ox, attac impa Successi bility c ability c ab	YM ht ity ity ity ity ful an to to tly S) as or YM as or YM as sor yM as se ty, s). or:	236626. ml		
NA	19-10-2017	4.3	Vuln Virtu Virtu Core is aff explo high to th VM com Virtu is in may addit attac resul causs repe of On unau delet Virtu	tional ks of t lt in u	y in compo- suppor suppor vulne ged att tructu Box While While VM Vi: gnifica produ this v nautho hang crash I Virtu d up s to so acces	the O onent (subco ted ve to 5.1. erabilit acker v ure whe Execut Oracle the vul rtualBo ntly ulneral orized or f (comp ualBox date, me of 0 sible	racle V of Orac mponen rsion th 30. Eas y allow vith log ere Orac eutes eutes with log ere Orac eutes bility c ability c ability c ability requent lete DO as well insert Dracle V data a	cle w nt: e.a nat hr ily /s ws ac on cp cle 17 to 32 /M ht ity ks act ful an to tly S) as or /M	tp://w w.oracl com/tec network security- lvisory/ puoct20 7- 236626. cml	VI-	RA-VM 117/
CV Scoring Scale (C	VSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type CSRF-Cross Site Rec Injection; XSS- Cros	quest Forgery; Dir	. TravDir	rectory	Traversal	; DoS-D	enial of S	Service; N	A- Not A	pplicable;	Sql-SQL	

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID Patch NCIIPC ID
Web Applicatio	ons Desktop In	Ŭ	
NA	19-10-2017	5.8	Vulnerability in the Oracle Web Applications Desktop Integrator component of Oracle E-Businesshttp://wA-ORA- WEB A- e.com/tccSuite (subcomponent: Application Service). Supported versions that are affected are 12.1.1, 12.1.2,
Webcenter Con	itent		
NA	19-10-2017	5.8	Vulnerability in the Oracle http://w A-ORA-
CV Scoring Scale (C	VSS)	0-1	1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10
Vulnerability Type CSRF-Cross Site Rec Injection; XSS- Cros	uest Forgery; Dir	. TravDir	rectory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL

Vulnerability	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
<u>Type(s)</u>	Date		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.oracl e.com/tec hnetwork /security- advisory/ cpuoct20 17- 3236626. html	WEBCE- 011117/ 273
Webcenter Site	'S				
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://w ww.oracl e.com/tec hnetwork /security- advisory/ cpuoct20 17- 3236626. html	A-ORA- WEBCE- 011117/ 274
CV Scoring Scale (CV	VSS)	0-1	1-2 2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10
Vulnerability Type((s): Juest Forgery; Dir	. TravDir	ectory Traversal; DoS-Denial of Service; NA- N	ot Applicable; S	ql-SQL

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 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</a 		
Weblogic Serve	r		CVE ID . CVE-2017-10035		
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://w ww.oracl e.com/tec hnetwork /security- advisory/ cpuoct20 17- 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://w ww.oracl e.com/tec hnetwork /security- advisory/ cpuoct20	A-ORA- WEBLO- 011117/ 276
CV Scoring Scale (CV		0-1	1-2 2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
	Dute		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).	17- 3236626. html	
NA	19-10-2017	4.3	CVE ID : CVE-2017-10152VulnerabilityintheOracleWebLogicServercomponentofOracleFusionMiddleware(subcomponent:WLS-WebServices).Supported versionsthatareaffectedare10.3.6.0.0,12.1.3.0.0,12.2.1.1.0and12.2.1.2.0.DifficulttoexploitvulnerabilityallowsunauthenticatedattackerwithnetworkaccessviaHTTPtocompromiseOracleWebLogicServer.Successfulattacksofthisvulnerabilitycauseunauthorizedabilitytounauthorizedabilitytocauseahangorfrequentlyrepeatablecrash(completeDOS)ofOracleWebLogicServer.CVSSScore5.9(AvailabilityMescoreSiltyN/UI:N/A:H).CVSSVector:(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://w ww.oracl e.com/tec hnetwork /security- advisory/ cpuoct20 17- 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://w ww.oracl e.com/tec hnetwork /security- advisory/ cpuoct20 17- 3236626.	A-ORA- WEBLO- 011117/ 278
CV Scoring Scale (CV		0-1	1-2 2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

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://w ww.oracl e.com/tec hnetwork /security- advisory/ cpuoct20 17- 3236626. html	A-ORA- WEBLO- 011117/ 279
Paessler	Voniton				
Prtg Network M Execute Code	19-10-2017	6.5	PRTGNetworkMonitor17.3.33.2830allowsremoteauthenticatedadministratorstoExecutearbitrarycodebyuploadingaexefileandproceedinginspiteoftheerrormessage.CVE ID : CVE-2017-15651	https://m edium.co m/stolabs /security- issue-on- prtg- network- manager- ada65b45 d37b	A-PAE- PRTG - 011117/ 280
Phpjabbers Rate Me					
CV Scoring Scale (C	VSS)	0-1	1-2 2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10
Vulnerability Type CSRF-Cross Site Rec Injection; XSS- Cros	uest Forgery; Dir	. TravDir	ectory Traversal; DoS-Denial of Service; NA- N	ot Applicable; S	ql-SQL

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://gi thub.com /thorsten /phpMyF AQ/com mit/2d2a 85b59e05 8869d7cb cfe2d73fe d4a282f2 e5b	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://gi thub.com /thorsten /phpMyF AQ/com mit/5c3e 4f96ff0ef 6b91a3f0 aa64eb28 197c5cf5 435	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://gi thub.com /thorsten /phpMyF AQ/com mit/cb64 8f0d5690 b81647d d5c9efe9 42ebf6cce 7da9	A-PHP- PHPMY- 011117/2 84
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://gi thub.com /thorsten /phpMyF AQ/com mit/8676 18110feb	A-PHP- PHPMY- 011117/ 285
CV Scoring Scale (CV	VSS)	0-1	1-2 2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10
Vulnerability Type(CSRF-Cross Site Req Injection; XSS- Cross	quest Forgery; Dir	. TravDir	rectory Traversal; DoS-Denial of Service; NA- N	ot Applicable; S	ql-SQL

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				836e1684 35548d6c 2cbb7c65 eda3	
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://gi thub.com /thorsten /phpMyF AQ/com mit/fa26c 52384b0 10edaf60 c525ae5b 040f05da 9f77	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://gi thub.com /thorsten /phpMyF AQ/com mit/ef5a6 6df4bcfac c7573322 af33ce10c 30e0bb89 6	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://gi thub.com /thorsten /phpMyF AQ/com mit/ec8b 3cc37d05 b6625e24 916b8f72 53f83001 5b5f	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://gi thub.com /thorsten /phpMyF AQ/com mit/fadb 9a70b5f7 624a6926 b8834d5c	A-PHP- PHPMY- 011117/ 289
		0-1	1-2 2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID Patch NCIIPC ID
			6001c210 f09c
CSRF	22-10-2017	6.8	In phpMyFAQ before 2.9.9, there is Cross-Site Request Forgery (CSRF)https://giA-PHP-in admin/stat.ratings.php./thorsten011117/CVE ID : CVE-2017-15730/phpMyF290AQ/com mit/cce47f94375b50102ab4f210672231dbb854dd0d
CSRF	22-10-2017	6.8	In phpMyFAQ before 2.9.9, there is Cross-Site Request Forgery (CSRF) for adding a glossary.https://gi HPPMY-
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 APHP- thub.com /thorsten 011117/ /phpMyF 292 AQ/com mit/a249 b4645fb8 6f6a9fbe5 d2344ab1 cbdb906b 75c
Phpwcms	I		
Phpwcms	24.40.0045	2 =	
XSS	24-10-2017	3.5	phpwcms1.8.9hasXSSinhttps://giA-PHP-include/inc_tmpl/admin.edituser.tthub.comPHPWC-mpl.phpand/slackero011117/include/inc_tmpl/admin.newuser.t/phpwcm293mpl.phpviatheusernamenew_login) field./90ee94a/90ee94aCVE ID : CVE-2017-15872474b37919161f8112f9e36c12f9e36c/
CV Scoring Scale (C	VSS)	0-1	1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10
Vulnerability Type CSRF-Cross Site Rec Injection; XSS- Cros	uest Forgery; Dir	. TravDir	rectory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL

Vulnerability Type(s)	Publish Date	CVSS		Desc	riptior	n & CVI	EID		Patc	h	NCII	PC ID
JT-(-)									53ad7 2f	049		
Post Highlights		-	-								•	
Post Highlights			1								1	
XSS	16-10-2017	4.3	plug allov arbi the actio	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						//w ess. ugi st- st- shts elo	A-P0 POS 011 294	
Qemu												
Qemu												
DoS	16-10-2017	2.1	hw/ allor user (out Qem rela	mode4a (display) w local rs to car -of-bou nu proc ted to da (ID : CV	/cirrus OS use a nds w ess cra st calcu	s_vga.c guest denial rrite ac ash) vi ılation.	in Qer privileg of servi ccess a a vecto	nu ged ice nd	https:/ ugzilla dhat.co /show g.cgi?io 50129	.re om _bu d=1	A-QI QEM 0111 295	
Radare												
Radare2												
DoS Overflow	16-10-2017	6.8	func libr, rada atta serv and have a cra CVE	ckers t vice (r_r applica e unspe afted EL ID : CV	mat/e .0.0 o cau ead_le tion cr cified F file. E-201	lf/elf.c allows se a 16 inva rash) o other i 7-1538	remo denial alid wr r possil mpact y 85	in in ote of ite oly via	https:/ thub.co /radar adare2 sues/8 5	om e/r 2/is 868	296	AR- 117/
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://thub.co /radar adare2 ommit 4ded31 5b826 4b5a90 ab32ec 9d9e5	om e/r 2/c /4 ff3 4f5 00c c48	A-RA RAD 0112 297	
NA	27-10-2017	6.8	In	radare	2 2.0	.1, an	integ	ger	https:/		A-RA	AD-
		0.1	1 0	2.2	2.4				7	0	0.0	0.40
CV Scoring Scale (CV	VSS)	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/r adare2/c ommit/c6 d0076c92 4891ad99 48a62d89 d0bcdaf9 65f0cd	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://w ww.redmi ne.org/iss ues/2419 9	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://w ww.redmi ne.org/iss ues/2550 3	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://w ww.redmi ne.org/pr ojects/re dmine/wi ki/Securit y_Advisor ies	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://w ww.redmi ne.org/pr ojects/re dmine/wi ki/Securit y_Advisor ies	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://w ww.redmi ne.org/pr ojects/re dmine/wi ki/Securit y_Advisor ies	A-RED- REDMI- 011117/ 303
XSS	17-10-2017	4.3	In Redmine before 3.2.8, 3.3.x 1-2 2-3 3-4 4-5 5-6 0	https://gi	A-RED-
CV Scoring Scale (C	VSS) (s):	0-1	1-2 2-3 3-4 4-5 5-6	0-7 7-8	8-9 9-10

CSRF-Cross Site Request Forgery; Dir. Trav.-Directory 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
	2000		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/ 94f7cfbf9 9002834 8b92625 78acbc53 a94fce44 8	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://w ww.redmi ne.org/pr ojects/re dmine/wi ki/Securit y_Advisor ies	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://w ww.redmi ne.org/iss ues/2379 3	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://w ww.redmi ne.org/iss ues/2380 3	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://w ww.redmi ne.org/iss ues/2441 6	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://w ww.redmi ne.org/iss ues/2430 7	A-RED- REDMI- 011117/ 309
CV Scoring Scale (CV		0-1	1-2 2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Vulnerability Type(s)	Publish Date	CVSS		Descr	iption	n & CVF	EID		Patch	NCI	IPC ID
	2400		impa CVE	act. ID : CVI	E-201'	7-1557	' 5				
SAP											
Customer Relat	-		1	- 1				. 1			1.5
XSS	16-10-2017	4.3	SAP Secu	Java adı CRM ł urity Not ID : CVI	nas XS e 2478	SS. Thi 8964.	s is S		NA	CUS	AP- STO- 117/
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	CUS	AP- STO- 117/
Softwarepublic	со										
E-sic											
XSS	23-10-2017	4.3	requ the i	exists lastro/ir lester's nome pa ID : CVI	ndex.p regist ramet	hp URI ration ær.	(aka t area)	the	NA	SIC	.117/
Sql	23-10-2017	6.5	pass the /res	Injectio word r cpfcnp et URI). ID : CVI	eset j par	parame ameter	eter (a to t	aka	NA	SIC	.117/
Sql	16-10-2017	7.5	the esicl (aka	E-Sic 1.0 allows SQL injection via					NA	SIC	117/
Sql	23-10-2017	7.5	the esicl p (al	Injectio f livre/res ka the zi ID : CVI	pa /trito p code	aramete inc/bu e search	er scacep. 1 script	to ph).	https://w ww.explo t- db.com/e xploits/4 2982/	i SIC 011	117/
Soundexchang	e								,		
Sound Exchang	ie										
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.					the ind ted of	https://b ugzilla.re dhat.com /show_bu g.cgi?id=1 500553	SOU 011 1 316	0U- JND- 117/
CV Scoring Scale (CV	VSS)	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://b ugzilla.re dhat.com /show_bu g.cgi?id=1 500570	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://b ugzilla.re dhat.com /show_bu g.cgi?id=1 500554	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://s ourceforg e.net/p/s ox/bugs/ 298/	A-SOU- SOUND- 011117/ 319
Store Locator I	Project				
Store Locator	16 10 2017	7 6		DI A	A 6700
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://gi thub.com /thefore man/fore man/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 (C Vulnerability Type(-	0-1	1-2 2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10
	uest Forgery; Dir	. TravDir	ectory Traversal; DoS-Denial of Service; NA- N	ot Applicable; S	ql-SQL

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
	Dute		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	https://a ccess.red hat.com/s ecurity/v ulnerabili ties/krac	A-WPA- WPA/W- 011117/ 323
			replay, decrypt, or spoof frames. CVE ID : CVE-2017-13077	ks	
Xnview				l	<u> </u>
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!LdrpResCompare ResourceNames+0x0000000000 00150." CVE ID : CVE-2017-15803	https://gi thub.com /wlinzi/s ecurity_a dvisories /tree/ma ster/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!LdrpResCompare ResourceNames+0x0000000000	https://gi thub.com /wlinzi/s ecurity_a dvisories /tree/ma ster/CVE- 2017- 15802	A-XNV- XNVIE- 011117/ 325
CV Scoring Scale (CV		0-1	1-2 2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Vulnerability	Publish Data	CVSS	Description & CVE ID	Patch	NCIIPC ID
Type(s)	Date		00087."		
			CVE ID : CVE-2017-15802		
DoS Overflow	22-10-2017	6.8	XnView Classic for Windows	https://gi	A-XNV-
D03 Overnow	22-10-2017	0.0	Version 2.43 allows attackers to	thub.com	XNVIE-
			cause a denial of service or	/wlinzi/s	011117/
			possibly have unspecified other	ecurity_a	326
			impact via a crafted .dll file that is	dvisories	520
			mishandled during an attempt to	/tree/ma	
			render the DLL icon, related to	ster/CVE-	
			"Data from Faulting Address	2017-	
			controls Branch Selection starting	15801	
			at	10001	
			ntdll_77310000!LdrpResSearchRe		
			sourceInsideDirectory+0x000000		
			000000029e."		
			CVE ID : CVE-2017-15801		
DoS Execute	22-10-2017	6.8	XnView Classic for Windows	https://gi	A-XNV-
Code			Version 2.43 allows attackers to	thub.com	XNVIE-
Overflow			Execute arbitrary code or cause a	/wlinzi/s	011117/
			denial of service via a crafted .dwg	ecurity_a	327
			file, related to a "User Mode Write	dvisories	
			AV starting at	/tree/ma	
			CADImage+0x00000000000048e7	ster/CVE-	
			." CVE ID : CVE-2017-15789	2017-	
				15789	
DoS Execute	22-10-2017	6.8	XnView Classic for Windows	https://gi	A-XNV-
Code			Version 2.43 allows attackers to	thub.com	XNVIE-
Overflow			Execute arbitrary code or cause a	/wlinzi/s	011117/
			denial of service via a crafted .dwg	ecurity_a	328
			file, related to a "User Mode Write	dvisories	
			AV starting at	/tree/ma	
			CADImage+0x0000000000002d83	ster/CVE-	
				2017-	
	22 10 2017	()	CVE ID : CVE-2017-15788	15788	A 375137
DoS Execute	22-10-2017	6.8	XnView Classic for Windows	https://gi	A-XNV-
Code Overflow			Version 2.43 allows attackers to Execute arbitrary code or cause a	thub.com	XNVIE-
Overnow				/wlinzi/s	011117/ 329
			denial of service via a crafted .dwg file, related to a "Data	ecurity_a dvisories	347
			Executeution Prevention Violation	/tree/ma	
			starting at	ster/CVE-	
			xnview+0x0000000000580063."	2017-	
			CVE ID : CVE-2017-15787	15787	
DoS Overflow	22-10-2017	6.8	XnView Classic for Windows	https://gi	A-XNV-
		0.0	Version 2.43 allows attackers to	thub.com	XNVIE-
ļ			cause a denial of service or	/wlinzi/s	011117/
				,, 5	
CV Scoring Scale (CV		0-1	1-2 2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

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

Vulnerability Type(s)	Publish Date	CVSS		Des	criptio	n & CV	EID		Patch	NCIII	PC ID
			impa relat start CADI ."	et vi ed to ing mage	a a ci a "Read	rafted Access	001a78d	e, dv on /tr at ste lb 20	urity_a isories ree/ma er/CVE- 17- 5786	330	
DoS Execute Code Overflow	22-10-2017	6.8	XnVi Versi Exec denia file, Prev start 0x00 CADI	ew ion 2 ute an al of s relate entior ing a 0000 image	Classic 43 allo bitrary ervice d to a 1 Viola t Unkr 000000	for ows at r code o via a cr "Data tion n own S 00000 c 000000	Windov tackers or cause afted dw Executic ear NUI Symbol alled fro 00286a7	to th a /w /g ec on dv L /tr @ ste m 20	tps://gi ub.com vlinzi/s urity_a isories ree/ma er/CVE- 017- 5785	A-XN XNVI 0111 331	E-
DoS Execute Code Overflow	22-10-2017	6.8	Exec denia file, Instr xnvie	ion 2 ute an al of s rela uction ew+03	.43 allo bitrary ervice v ited t i Viola	ows at code o via a cr co an tion s 000003	tarting 370074."	to th a /w /g ec al dv at /t ste 20	tps://gi ub.com vlinzi/s urity_a risories ree/ma er/CVE- 017- 5784	A-XN XNVI 0111 332	E-
DoS Overflow	22-10-2017	6.8	cause possi impa relat Addr start CADI	ion 2 e a ibly l ict vi ed to ress co ing mage	denial nave u a a ci Data ontrols	of s nspecif rafted a from Branch 000000	ied oth .dwg fil Faultin Selectio 00285ce	vs ht to th or /w er ec e, dv ng /tr on ste at 20	tps://gi ub.com vlinzi/s urity_a risories ree/ma er/CVE- 017- 5783	A-XN XNVI 0111 333	E-
DoS Execute Code Overflow	22-10-2017	6.8	XnVi Versi Exec denia file, 1 AV CADI	ew ion 2 ute an al of s relate mage	Classic .43 allo bitrary ervice v d to a " star	for ows at code via a cr User M ting 000000	Windov tackers or cause afted .dv ode Wri 000032e	to th a /w /g ec te dw at /t b ste 20	tps://gi ub.com vlinzi/s urity_a risories ree/ma er/CVE- 17- 5782	A-XN XNVI 0111 334	E-
DoS Execute	22-10-2017	6.8 0-1	XnVi	ew 2-3	Classic	for	Windov	vs ht	tps://gi	A-XN 8-9	
CV Scoring Scale (CVSS) Vulnerability Type(s):		0-1	1-2	2-3	3-4	4-5	5-0	0-7	7-8	0-9	9-10

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID Patch NCIIPC ID
Code	Dale		Version 2.43 allows attackers to thub.com XNVIE-
Overflow			Execute arbitrary code or cause a /wlinzi/s 011117/
			denial of service via a crafted .dwg ecurity_a 335
			file, related to a "Read Access dvisories
			Violation on Control Flow starting /tree/ma
			at ster/CVE-
			CADImage+0x000000000286a76 2017-
			." CVE ID : CVE-2017-15781 15781
DoS Overflow	22-10-2017	6.8	XnView Classic for Windows https://gi A-XNV-
			Version 2.43 allows attackers to thub.com XNVIE-
			cause a denial of service or /wlinzi/s 011117/
			possibly have unspecified other ecurity_a 336
			impact via a crafted .dwg file, dvisories
			related to a "Read Access Violation /tree/ma
			starting at ster/CVE-
			CADImage+0x000000000285dad 2017- ." CVE ID : CVE-2017-15780 15780
DoS Execute	22-10-2017	6.8	XnView Classic for Windows https://gi A-XNV-
Code	22-10-2017	0.0	Version 2.43 allows attackers to thub.com XNVIE-
Overflow			Execute arbitrary code or cause a /wlinzi/s 011117/
			denial of service via a crafted .dwg ecurity_a 337
			file, related to "Data from Faulting dvisories
			Address controls subsequent /tree/ma
			Write Address starting at ster/CVE-
			CADImage+0x0000000000034b0 2017-
			." CVE ID : CVE-2017-15779 15779
DoS Overflow	22-10-2017	6.8	XnView Classic for Windows https://gi A-XNV-
			Version 2.43 allows attackers to thub.com XNVIE-
			cause a denial of service or /wlinzi/s 011117/
			possibly have unspecified other ecurity_a 338
			impact via a crafted .dwg file, dvisories
			related to a "Read Access Violation /tree/ma
			starting at ster/CVE- CADImage+0x00000000285de7 2017-
			." CVE ID : CVE-2017-15778 15778
DoS Execute	22-10-2017	6.8	XnView Classic for Windows https://gi A-XNV-
Code		0.0	Version 2.43 allows attackers to thub.com XNVIE-
Overflow			Execute arbitrary code or cause a /wlinzi/s 011117/
			denial of service via a crafted .dwg ecurity_a 339
			file, related to a "User Mode Write dvisories
			AV near NULL starting at /tree/ma
			CADImage+0x000000000288750 ster/CVE-
			." 2017-
			CVE ID : CVE-2017-15777 15777
DoS Overflow	22-10-2017	6.8	XnView Classic for Windows https://gi A-XNV-
			Version 2.43 allows attackers to thub.com XNVIE-
	/SS)	0-1	1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10

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

	2-10-2017	6.8	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+0x000000000285ec1 ." CVE ID : CVE-2017-15776 XnView Classic for Windows Version 2.43 allows attackers to cause a denial of service or	/wlinzi/s ecurity_a dvisories /tree/ma ster/CVE- 2017- 15776 https://gi thub.com	011117/ 340 A-XNV-
DoS Overflow 22	2-10-2017	6.8	XnView Classic for Windows Version 2.43 allows attackers to		A-XNV-
			possibly have unspecified other impact via a crafted .dwg file, related to "Data from Faulting Address controls Branch Selection starting at CADImage+0x000000000259aa4 ." CVE ID : CVE-2017-15775	/wlinzi/s ecurity_a dvisories /tree/ma ster/CVE- 2017- 15775	XNVIE- 011117/ 341
DoS Execute 22 Code Overflow	2-10-2017	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+0x000000000221a9a ." CVE ID : CVE-2017-15774	https://gi thub.com /wlinzi/s ecurity_a dvisories /tree/ma ster/CVE- 2017- 15774	A-XNV- XNVIE- 011117/ 342
DoS Overflow 22	2-10-2017	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+0x00000000285d79 ." CVE ID : CVE-2017-15773	https://gi thub.com /wlinzi/s ecurity_a dvisories /tree/ma ster/CVE- 2017- 15773	A-XNV- XNVIE- 011117/ 343
DoS Overflow 22	2-10-2017	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+0x00000000285e9d ." CVE ID : CVE-2017-15772	https://gi thub.com /wlinzi/s ecurity_a dvisories /tree/ma ster/CVE- 2017- 15772	A-XNV- XNVIE- 011117/ 344
CV Scoring Scale (CVSS)	5)	0-1	1-2 2-3 3-4 4-5 5-6 (6-7 7-8	8-9 9-10

CSRF-Cross Site Request Forgery; Dir. Trav.-Directory 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/Iphor					
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://s upport.ap ple.com/ HT20811 2	A-APP- APPLE- 011117/ 345
Apple Tv/Iphor	ne Os:Mac Os Z	X:Watch		I	
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.	https://s upport.ap ple.com/ HT20814 4	A-APP- APPLE- 011117/ 346
			CVE ID : CVE-2017-7083		
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://s upport.ap ple.com/ HT20814 4	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://s upport.ap ple.com/ HT20814 4	A-APP- APPLE- 011117/ 348
CV Scoring Scale (CV	/\$\$)	0-1	1-2 2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

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

DoS Overflow 22 DoS Overflow 22	2-10-2017 2-10-2017	7.5	(application crash) or possibly have unspecified other impact. CVE ID : CVE-2017-7130 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 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	https://s upport.ap ple.com/ HT20814 4 https://s upport.ap ple.com/ HT20814 4	A-APP- APPLE- 011117/ 349 A-APP- APPLE- 011117/ 350
DoS Overflow 22			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 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	upport.ap ple.com/ HT20814 4 https://s upport.ap ple.com/ HT20814	APPLE- 011117/ 349 A-APP- APPLE- 011117/
	2-10-2017	7.5	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	upport.ap ple.com/ HT20814	APPLE- 011117/
DoS 22			cause a denial of service (application crash) or possibly have unspecified other impact. CVE ID : CVE-2017-7128		
	2-10-2017	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://s upport.ap ple.com/ HT20814 4	A-APP- APPLE- 011117/ 351
DoS Execute 22 Code Overflow Mem. Corr.	2-10-2017	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://s upport.ap ple.com/ HT20814 4	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)	Publish Date	CVSS	Desc	ription &	CVE ID		Patch	NCIIPC	ID
	Date		Executeute privileged denial of corruption) CVE ID : CV	context service via a craft	or cause (memo ed app.	а			
Apple Tv/Iphor									
Gain Information	22-10-2017	5	component. attackers to memory loo Fi traffic. CVE ID : CV	lucts. iOS OS before 1 efore 4 is a volves th . It might a o read data cations via	before 11 1 is affected affected. The "Wi-H allow remo from kern crafted W 116	is up ed. ple he HT Fi" 5 te lel Zi-	port.ap e.com/ 20811	A-APP- APPLE- 011117 353	
DoS Execute Code Overflow Mem. Corr.	22-10-2017	7.5	An issue wa Apple prod affected. tv(watchOS be issue inv component. attackers code in a cause a den corruption) traffic. CVE ID : CV	lucts. iOS OS before 1 efore 4 is volves th . It might a to Execut privileged nial of serv via cr	before 11 1 is affected affected. The "Wi-H allow remo te arbitra l context ice (memo afted Wi-	is up ed. ple he HT Fi" 5 te ry or ry	port.ap e.com/ 20811	A-APP- APPLE- 011117 354	
DoS Execute Code Overflow Mem. Corr.	22-10-2017	10	An issue wa Apple prod affected. tv(watchOS be issue inv component. attackers code in a cause a den corruption) traffic. CVE ID : CV	lucts. iOS OS before 1 efore 4 is volves th It might a to Execut privileged nial of serv via cr	before 11 1 is affected affected. The "Wi-H allow remo te arbitra l context ice (memo afted Wi-	is up ed. ple he HT Fi" 5 te ry or ry	ps://s port.ap e.com/ 20811	A-APP- APPLE- 011117 355	
DoS Execute Code Overflow Mem. Corr.	22-10-2017	10	component	lucts. iOS OS before 1 efore 4 is a volves tl . It might a	before 11 1 is affecte affected. T he "Wi-H	is up ed. ple he HT Fi" 5 te	ps://s port.ap e.com/ '20811	A-APP- APPLE- 011117 356	/
CV Scoring Scale (CV	VSS)	0-1	1-2 2-3	3-4 4	4-5 5-6	6-7	7-8	8-9	9-10
Vulnerability Type CSRF-Cross Site Rec Injection; XSS- Cros	quest Forgery; Dir	. TravDir	ectory Traversa	ll; DoS-Denia	l of Service; N	A- Not Ar	oplicable; S	Sql-SQL	

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
	batt		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://s upport.ap ple.com/ HT20811 5	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://s upport.ap ple.com/ HT20811 5	A-APP- APPLE- 011117/ 358
Apple Tv;Icloud	1/Iphone Os;M	lac Os X			
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://s upport.ap ple.com/ HT20814 4	A-APP- APPLE- 011117/ 359
Apple Tv;Icloud				h	
XSS	22-10-2017	4.3 0-1	An issue was discovered in certain	https://s	A-APP- 8-9 9-10
CV Scoring Scale (CV	-				
Vulnerability Type(CSRF-Cross Site Req Injection; XSS- Cros	juest Forgery; Dir	. TravDir	rectory Traversal; DoS-Denial of Service; NA- N	ot Applicable; S	ql-SQL

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
	butc		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.ap ple.com/ HT20814 2	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://s upport.ap ple.com/ HT20814 2	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://s upport.ap ple.com/ HT20814 2	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://s upport.ap ple.com/ HT20814 2	A-APP- APPLE- 011117/ 363
CV Scoring Scale (CV	VSS)	0-1	1-2 2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; 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://s upport.ap ple.com/ HT20811 3	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://s upport.ap ple.com/ HT20814 2	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://s upport.ap ple.com/ HT20814 2	A-APP- APPLE- 011117/ 366
CV Scoring Scale (C	VSS)	0-1	1-2 2-3 3-4 4-5 5-6 0	6-7 7-8	8-9 9-10

CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sc 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://s upport.ap ple.com/ HT20814 2	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://s upport.ap ple.com/ HT20814 2	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://s upport.ap ple.com/ HT20814 2	A-APP- APPLE- 011117/ 369
CV Scoring Scale (C	VSS)	0-1	1-2 2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	De	escriptio	n & CVE	ID		Patch	NCIIP	PC ID
DoS Execute Code Overflow Mem. Corr.	22-10-2017	6.8	Apple pr affected. affected. Window 12.7 on before 1 involves It allow Execute denial corruption	iCloud s is affect Windows 1 is aff the "Wel vs remo arbitrary of sen on and a fted web	iOS before before ced. iTun s is affec ected. T bKit" co te atta v code o rvice pplicatio	ore 11 7.0 es befo ted. tv The iss mpone ckers r cause (memo on cras	is u is p on H ore 2 7OS sue ent. to e a ory sh)	ttps://s pport.ap le.com/ T20814	A-APF APPL 01111 370	E-
DoS Execute Code Overflow Mem. Corr.	22-10-2017	6.8	An issue Apple pr affected. affected. Window 12.7 on before 1 involves It allow Execute denial corruptio	was disc roducts. Safari iCloud s is affect Windows 1 is affe the "Wel vs remo arbitrary of sen on and a fted web	iOS before before ced. iTun s is affec ected. T bKit" co te atta v code o rvice pplicatio	ore 11 7.0 es befo ted. tv The iss mpone ckers r cause (memo on cras	is u is p on H ore 2 7OS sue ent. to e a ory sh)	ttps://s pport.ap le.com/ T20814	A-APF APPL 01111 371	E-
DoS Execute Code Overflow Mem. Corr.	22-10-2017	6.8	An issue Apple pr affected. affected. Window 12.7 on before 1 involves It allow Execute denial corruptio	was disc roducts. Safari iCloud s is affect Windows 1 is affe the "Wel vs remo arbitrary of sen on and a rafted we	iOS before before ced. iTun s is affec ected. T bKit" con te attac v code o rvice pplicatio	ore 11 7.0 es befo ted. tv The iss mpone ckers r cause (memo on cras	is u is p on H ore 2 70S sue ent. to e a ory sh)	ttps://s pport.ap le.com/ T20814	A-APF APPL 01111 372	Е-
DoS Execute Code Overflow Mem. Corr.	22-10-2017	6.8	Apple praised.	was disc roducts. Safari iCloud	iOS befo before	ore 11 11	is u is p	ttps://s pport.ap le.com/ T20814	A-APF APPL 01111 373	Е-
		0-1	1-2 2-	3 3-4	4-5	5-6	6-7	7-8	8-9	9-10

Type(s)	Publish Date	CVSS		Desc	ription	ı & CVE	, ID		Patch	NCII	PC ID
			12.7 befo invo It a Exec deni corr via a	on Wi ore 11 olves th allows cute ar ial o ruption	ndows is affe e "Web remot bitrary f ser and ap d web s	ed. iTur is affec ected. 7 oKit" co te atta code o vice oplicatio site. CVE	cted. tvo The iss mpone ckers r cause (memo on cras	OS ue nt. to e a ery sh)			
DoS Execute Code Overflow Mem. Corr.	22-10-2017	6.8	An i App affec affec Win 12.7 befc invc It Exec deni corr via a	ssue w le proc cted. i dows is ore 11 olves th allows cute ar ial o ruption	as disco lucts. i Safari Cloud s affecto ndows is affe e "Web remot bitrary f ser and ap d web s	overed OS before before ed. iTur is affec ected. To oKit" co ce atta code o vice oplicatio site. CVE	ore 11 7.0 tes befo cted. tvo The iss mpone ckers r cause (memo on cras	is up is pla on HT ore 2 OS - ue - nt to - e a - ory - ch) -	tps://s oport.ap e.com/ T20814	A-AF APP 0112 374	
DoS Execute Code Overflow Mem. Corr.	22-10-2017	6.8	App affec affec Win 12.7 befc invo It Exec deni corr via a	le prod cted. cted. i dows is ore 11 olves th allows cute ar ial o uption	lucts. i Safari Cloud s affecto ndows is affe e "Web remot bitrary f ser and ap d web s	before ed. iTur is affec ected. T oKit" co ce atta code o	ore 11 7.0 tes befo cted. tvt The iss mpone ckers r cause (memo on cras	is up is pla on H7 ore 2 OS - ue - nt to - e a - ory - ch) -	tps://s port.ap e.com/ C20814	A-AF APP 0112 375	LE-
DoS Execute Code Overflow Mem. Corr.	22-10-2017	6.8	An i App affe affe Win 12.7 befc	ssue w le proc cted. cted. i dows is ' on Wi ore 11	as disco lucts. i Safari Cloud s affecto ndows is affe	overed OS before before ed. iTur is affec ected. T oKit" co	ore 11 7.0 nes befo cted. tv The iss	is up is pla on HT ore 2 OS ue	tps://s port.ap e.com/ r20814	A-AF APP 0112 376	LE-
CV Scoring Scale (CV		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	CVSS		Desc	ription	ı & CVE	ID		Patch	NCIII	PC ID
1990(0)			Exec a c corr via a	cuteute lenial uption	arbitra of se and ar d web s	e atta ry code rvice oplicatio site. CVE	e or cau (memo on cras	ise ory sh)			
DoS Execute Code Overflow Mem. Corr.	22-10-2017	6.8	An is Applaffect affect Win 12.7 befo invo It a Exect denii corr via a	ssue wa le proc cted. i cted. i dows is on Wi re 11 lves th allows cute arl al of uption	as disco lucts. i Safari Cloud affecto ndows is affe e "Web remot pitrary ser and ap d web s	overed OS before before ed. iTun is affec ected. To Kit" co e atta code o vice oplicatio site. CVE	ore 11 7.0 es befo ted. tv The iss mpone ckers r cause (memo on cras	is ur is pl on H' ore 2 OS sue nt. to e a ory sh)	tps://s oport.ap e.com/ T20814	A-AP APPL 0111 377	νE-
DoS Execute Code Overflow Mem. Corr.	22-10-2017	6.8	Appl affec affec Win 12.7 befo invo It a Exec deni corr via a	le proc cted. i dows is on Wi re 11 lves th allows cute arl al of uption	lucts. i Safari Cloud affecte ndows is affe e "Web remot pitrary ser and ap d web s	overed OS before before ed. iTum is affec ected. To Kit" co e atta code o vice oplicatio	ore 11 7.0 es befo ted. two The iss mpone ckers r cause (memo on cras	is up is pl on H' ore 2 OS sue nt. to e a ory sh)	ttps://s oport.ap e.com/ T20814	A-AP APPL 0111 378	LΕ-
DoS Execute Code Overflow Mem. Corr.	22-10-2017	6.8	An is Appl affec affec Win 12.7 befo invo It a Exec deni corr	ssue wa le proc cted. s cted. i dows is on Wi re 11 lves th allows cute arl al of uption	as disco lucts. i Safari Cloud affecto ndows is affe e "Web remot pitrary ser and ap	overed before before ed. iTun is affec ected. T oKit" co e atta code o vice oplicatio	ore 11 7.0 es befo ted. tv The iss mpone ckers r cause (memo	is up is pl on H' ore 2 OS sue nt. to e a ory	tps://s oport.ap e.com/ T20814	A-AP APPL 0111 379	νE-
CV Scoring Scale (CV		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			via a crafted web site.CVE ID :CVE- 2017-7081		
Icloud;Safari/I	phone 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://s upport.ap ple.com/ HT20814 2	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.	http://xe nbits.xen. org/xsa/a dvisory- 162.html	A-QEM- QEMU/- 011117/ 381
			CVE ID : CVE-2015-7504		
Apple		U	PERATING SYSTEM(OS)		
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://s upport.ap ple.com/ HT20811 2	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://s upport.ap ple.com/ HT20811 2	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; Di Injection; XSS- Cross Site Scripting;	r. TravI	Directory	Traversa	al; DoS-Do	enial of S	ervice; N	A- Not Ap	plicable;	Sql-SQL	

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://s upport.ap ple.com/ HT20811 2	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://s upport.ap ple.com/ HT20811 2	0-APP- IPHON- 011117/3 85
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://s upport.ap ple.com/ HT20811 2	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://s upport.ap ple.com/ HT20811 2	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://s upport.ap ple.com/ HT20811 2	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://s upport.ap ple.com/ HT20811 2	O-APP- IPHON- 011117/ 389
CV Scoring Scale (CV		0-1	1-2 2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-S Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
1900(8)	2000		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://s upport.ap ple.com/ HT20811 2	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://s upport.ap ple.com/ HT20811 2	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://s upport.ap ple.com/ HT20811 2	O-APP- IPHON- 011117/ 392
Iphone Os;Mac	Os X				<u> </u>
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://s upport.ap ple.com/ HT20814 4	O-APP- IPHON- 011117/ 393
Mac Os X			CVE ID : CVE-2017-7078		
Bypass	22-10-2017	2.1	An issue was discovered in certain Apple products. macOS before	https://s upport.ap	O-APP- MAC O-
CV Scoring Scale (C	VSS	0-1		6-7 7-8	8-9 9-10
Vulnerability Type	(s): quest Forgery; Dir	. TravDir	ectory Traversal; DoS-Denial of Service; NA- N	ot Applicable; S	ql-SQL

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
<u>- Type(s)</u>	Date		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/ HT20816 5	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://s upport.ap ple.com/ HT20816 5	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://s upport.ap ple.com/ HT20814 4	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://s upport.ap ple.com/ HT20814 4	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://s upport.ap ple.com/ HT20814 4	O-APP- MAC O- 011117/ 398
		0-1	1-2 2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-S Injection; XSS- Cross Site Scripting;

Type(s)	Publish Date	CVSS		escription		Patch	NCIII	PC ID		
				te attac ion Firewa CVE-201 7	ad					
Bypass	22-10-2017	4.3	Apple 1 10.13 involves compone bypass restrictio	was disco products. is affecte the "IO ent. It allo intended ons via a c CVE-201	ore up ue ple ly" HT	tps://s port.ap e.com/ T20814	0-AP MAC 0111 399	0-		
Bypass	22-10-2017	4.3	Apple 1 10.13 involves compone attacker settings circumst incorrec setting a	in	ore up ue ple ill" HT ote 4 ed tic ng	tps://s port.ap e.com/ 720814	0-AP MAC 0111 400	0-		
DoS	22-10-2017	4.3	Apple 1 10.13 involves compone cause a crafted a	ent. It allo denial o	ore up ue ple ox" HT to 4	tps://s port.ap e.com/ 20814	0-AP MAC 0111 401	0-		
Bypass Gain Information	22-10-2017	5	Apple 1 10.13 involves allows r an inten remote setting, a an e-ma via an H' CVE ID :	was disco products. is affecte the "Mail emote atta ded off va content and consec il recipie TML email CVE-201	ore up ue ple It HT ass 4 ad es" ver ss,	tps://s port.ap e.com/ 520814	0-AP MAC 0111 402	0- 17/		
DoS Execute Code Overflow Mem. Corr.	22-10-2017	6.8	An issue Apple pr	was disco roducts. X The issu compone attacker	overed i code be ie invo nt. It	in certa efore 9 olves t	is up he ple ws HT	tps://s port.ap e.com/ F20810	0-AP MAC 0111 403	0-
CV Scoring Scale (CV	VSS)	0-1	1-2 2-	-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
	2000		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://s upport.ap ple.com/ HT20814 4	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://s upport.ap ple.com/ HT20814 4	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://s upport.ap ple.com/ HT20814 4	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://s upport.ap ple.com/ HT20814 4	O-APP- MAC O- 011117/ 407
DoS	22-10-2017	7.5	An issue was discovered in certain	1 //	O-APP-
CV Scoring Scale (CV		0-1	1-2 2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Injection; XSS- Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE IDPatchNCIIPC ID
			Appleproducts.macOSbeforeupport.apMAC 0-10.13isaffected.Theissueple.com/011117/involvesthethird-party"file"HT20814408product.Versionsbefore5.304allow remote attackers to cause a4408408crash)orpossiblyhave4unspecified other impact.4408408
DoS	22-10-2017	7.5	An issue was discovered in certainhttps://sO-APP-Apple products. macOS beforeupport.apMAC O-10.13 is affected. The issueple.com/011117/4involves the third-party "file"HT2081409product. Versions before 5.304allow remote attackers to cause a4allow remote attackers to cause ainvolvesinvolvestenial of service (applicationinvolvesinvolvestrash) or possibly haveinvolvesinvolvestenial of tenial of tenial of tenialinvolvesinvolvestenial of tenialinvolvesinvolvestenialtenial<
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 ple.com/0-APP- MAC 0- 011117/ HT20814involves the "IOFireWireFamily" component. It allows attackers to privileged context or cause a denial of service (memory corruption) via a crafted app.4
Fortinet			
<u>Fortios</u> DoS	27-10-2017	4	ADenialofService(DoS)https://foO-FOR-vulnerabilityinFortinetFortiOSrtiguard.cFORTI-5.4.0to5.4.5allowsanom/psirt/011117/authenticatedusertocausetheFG-IR-17-411webGUItobetemporarily2061000unresponsive,viapassingaspeciallyraftedpayloadto1000yearams'parameteroftheJSON1000100010001000webAPI.LLLLLLLLLCVE ID : CVE-2017-14182LLLLLLLLLL
Execute Code XSS	27-10-2017	4.3	ACross-Site-Scripting(XSS)https://foO-FOR-vulnerability in Fortinet FortiOSrtiguard.cFORTI-5.4.0 to5.4.5 and5.6.0 allows aom/psirt/011117/remote unauthenticated attackerFG-IR-17-412toExecuteute arbitrary javascript113113
CV Scoring Scale (C	VSS)	0-1	1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10
Vulnerability Type CSRF-Cross Site Rec Injection; XSS- Cros	quest Forgery; Dir	. TravDir	rectory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID Patch NCIIPC ID
	Dute		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 ALSAhttp://wO-LIN-subsystem in the Linux kernelww.kerneLINUX-before 4.13.8 allows local users tol.org/pub011117/cause a denial of service (use- after-free) or possibly have/linux/ke413after-free) or possibly havernel/v4.x/changeLcrafted /dev/snd/seq ioctl calls, sound/core/seq/seq_clientmgr.cog-4.13.8and sound/core/seq/seq_ports.c.CVE ID : CVE-2017-15265
Oracle			
Integrated Light			
Gain Information	19-10-2017	4	VulnerabilityintheOraclehttp://wO-ORA-Integrated LightsOutManagerww.oraclINTEG-(ILOM)component of Oracle Sune.com/tec011117/SystemsProductsSuitehnetwork414(subcomponent:System/security-Management).Thesupportedadvisory/version that is affected is Prior tocpuoct203.2.6.Easilyexploitableprivileged attacker with network17-vulnerabilityallowshigh3236626.htmlprivileged attacker with networkhtmlaccess viaHTTP to compromiseOracleIntegratedOracleIntegrated LightsUtManagerManager(ILOM).Successfulattacks of this vulnerability canresult in unauthorized read accessto a subset of OracleIntegratedLightsOutManager(ILOM)accessibledata.CVSSVector:(CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N).CVE ID:CVE-2017-10194
DoS	19-10-2017	7.5	VulnerabilityintheOraclehttp://wO-ORA-IntegratedLightsOutManagerww.oraclINTEG-(ILOM)componentofOracleSune.com/tec011117/SystemsProductsSuitehnetwork415(subcomponent:System/security-
CV Scoring Scale (CV	vss)	0-1	1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10
Vulnerability Type((s): quest Forgery; Dir	. TravDir	rectory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL

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).	advisory/ cpuoct20 17- 3236626. html	
NA	19-10-2017	7.8	CVE ID : CVE-2017-10265VulnerabilityintheOracleIntegratedLightsOutManager(ILOM)componentofOracleSunSystemsProductsSuiteSuite(subcomponent:SystemManagement).Thesupportedversionthat is affected isPrior to3.2.6.Easilyexploitablevulnerabilityallowsunauthenticatedattackerwithnetworkaccessvia HTTPtocompromiseOracleIntegratedLightsUnerabilitycansuccessfulattacksofthisvulnerabilitycansuccessfulattacksofthisvulnerabilitycancompromiseoracleIntegratedabilitytocauseahangorfrequentlyrepeatablecrash(completeDOS)ofOracleIntegratedLightsOutManager	http://w ww.oracl e.com/tec hnetwork /security- advisory/ cpuoct20 17- 3236626. html	0-0RA- INTEG- 011117/ 416
CV Scoring Scale (C	-	0-1		6-7 7-8	8-9 9-10
Vulnerability Type CSRF-Cross Site Rec Injection; XSS- Cros	quest Forgery; Dir	. TravDir	rectory Traversal; DoS-Denial of Service; NA- N	ot Applicable; S	ql-SQL

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID Patch NCIIPO	C ID
			(ILOM). CVSS 3.0 Base Score 7.5(Availability impacts). CVSSVector:(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	1			
NA	19-10-2017	6.3	Vulnerability in the Sun ZFS Storage Appliance Kit (AK) ww.oracl0-ORA SOLAR e.com/tecStorage Appliance Kit (AK) roducts Suite (subcomponent: Products Suite (subcomponent: 	{ -
XEN				
<u>XEN</u> 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 advisory- advisory- 244.htmlO-XEN 	
DoS Gain Privileges	18-10-2017	4.6	An issue was discovered in Xen https://x O-XEN- through 4.9.x allowing x86 guest enbits.xen XEN- OS users to cause a denial of .org/xsa/ 01111	
CV Scoring Scale (C	VSS)	0-1	1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9	9-10
Vulnerability Type	(s): quest Forgery; Dir	. TravDir	rectory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL	

-2017 4.9 -2017 4.9 -2017 4.9	 service (hypervisor crash) or possibly gain privileges because MSI mapping was mishandled. CVE ID : CVE-2017-15590 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 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 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 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 	advisory- 237.html https://x enbits.xen .org/xsa/ advisory- 235.html https://x enbits.xen .org/xsa/ advisory- 242.html https://x enbits.xen .org/xsa/ advisory- 238.html	419 O-XEN- XEN- 011117/ 420 O-XEN- XEN- 011117/ 421 O-XEN- XEN- 011117/ 422
-2017 4.9	 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 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 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. 	enbits.xen .org/xsa/ advisory- 235.html https://x enbits.xen .org/xsa/ advisory- 242.html https://x enbits.xen .org/xsa/ advisory-	XEN- 011117/ 420 O-XEN- XEN- 011117/ 421 O-XEN- XEN- 011117/
	 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 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. 	enbits.xen .org/xsa/ advisory- 242.html https://x enbits.xen .org/xsa/ advisory-	XEN- 011117/ 421 O-XEN- XEN- 011117/
-2017 4.9	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.	enbits.xen .org/xsa/ advisory-	XEN- 011117/
	UVE ID : UVE-201/-15591		
-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://x enbits.xen .org/xsa/ advisory- 240.html	O-XEN- XEN- 011117/ 423
-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 OS;Application (OS/A)	https://x enbits.xen .org/xsa/ advisory- 243.html	O-XEN- XEN- 011117/ 424
0-1		6-7 7-8	8-9 9-10
		privileges via crafted page-table stacking. CVE ID : CVE-2017-15595 -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 OS;Application (OS/A)	privileges via crafted page-table stacking. CVE ID : CVE-2017-15595-20177.2An 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-2017-15592https://x enbits.xen .org/xsa/ advisory- 243.htmlOS;Application (OS/A)0-11-22-33-44-55-66-77-8

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Apple/Apple					
Iphone Os/Safa	ari				
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://s upport.ap ple.com/ HT20811 6	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://s upport.ap ple.com/ HT20811 6	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. TravDirectory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;												