Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Application (A)					
BMC					
Remedy Action Request System BMC Remedy Action Request System (ARS) is a proprietary application server developed initially by Remedy Corp and acquired by BMC Software in 2002.					
Denial of Service; Execute Code; Gain Information	21-12-2016	5	Remedy AR System Server in BMC Remedy 8.1 SP 2, 9.0, 9.0 SP 1, and 9.1 allows attackers to reset arbitrary passwords via a blank previous password. **REFERENCE: CVE-2016-2349**	NA	A-BMC-REMED-030116/01
NA	21-12-2016	5	Remedy AR System Server in BMC Remedy 8.1 SP 2, 9.0, 9.0 SP 1, and 9.1 allows attackers to reset arbitrary passwords via a blank previous password. **REFERENCE: CVE-2016-2349**	NA	A-BMC-REMED-030116/02
Bundler					
Bundler Bundler provides a consistent environment for Ruby projects by tracking and installing the exact gems and versions that are needed.					
NA	22-12-2016	7.5	Bundler 1.x might allow remote attackers to inject arbitrary Ruby code into an application by leveraging a gem name collision on a secondary source. NOTE: this might overlap CVE-2013-0334. **REFERENCE: CVE-2016-7954**	NA	A-BUN-BUNDL-030116/03
Cisco					
Cloud-Center Orchestrator Cisco Cloud-Center Orchestrator is a cloud-specific multitenant orchestration tier.					
NA	26-12-2016	10	Vulnerability in the Docker Engine configuration of Cisco Cloud-Center Orchestrator (CCO; formerly CliQr) could allow an unauthenticated, remote attacker to install Docker containers with high	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-	A-CIS-CLOUD-030116/04

			privileges on the affected system. Affected Products: This vulnerability affect all releases of Cisco Cloud-Center Orchestrator (CCO) deployments where the Docker Engine TCP port 2375 is open on the system and bound to local address 0.0.0.0 (any interface). **REFERENCE: CVE-2016-9223**	20161221-cco	
Intercloud Fabric Intercloud Fabric for Providers is ideal for service providers that want to offer hybrid cloud deployment models and be a part of the Intercloud Fabric ecosystem.					
NA	26-12-2016	6.5	Vulnerability in Cisco Intercloud Fabric for Business and Cisco Intercloud Fabric for Providers could allow an unauthenticated, remote attacker to connect to the database used by these products. More Information: CSCus99394. Known Affected Releases: 7.3(0)ZN(0.99). **REFERENCE: CVE-2016-9217**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161221-icf	A-CIS-INTER-030116/05
Jabber Guest Cisco Jabber Guest is deployed as a virtual server and requires a VMware server to act its host. The server operating system is CentOS. Cisco Jabber Guest is an on-premises deployment: all services are set up, managed, and maintained on your corporate network.					
NA	26-12-2016	6.4	Vulnerability in the Cisco Jabber Guest Server could allow an unauthenticated, remote attacker to initiate connections to arbitrary hosts. More Information: CSCvc31635. Known Affected Releases: 10.6(9). Known Fixed Releases: 11.0(0). **REFERENCE: CVE-2016-9224**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161221-jabber	A-CIS-JABBE-030116/06
Dotcms					
Dotcms dotCMS is an Open Source Content Management System (CMS), built on leading Java technology and open standards.					
Execute Code; SQL Injection	19-12-2016	7.5	SQL injection vulnerability in the REST API in dotCMS before	https://github.com/dotCM	A-DOT-DOTCM-

			3.3.2 allows remote attackers to execute arbitrary SQL commands via the stName parameter to api/content/save/1. **REFERENCE: CVE-2016-2355**	S/core/issues/8848	030116/07
Execute Code; SQL Injection	19-12-2016	7.5	SQL injection vulnerability in the REST API in dotCMS before 3.3.2 allows remote attackers to execute arbitrary SQL commands via the stName parameter to api/content/save/1. **REFERENCE: CVE-2016-2355**	https://github.com/dotCMS/core/issues/8848	A-DOT-DOTCM-030116/08
Ffmpeg					
Ffmpeg ffmpeg is a very fast video and audio converter that can also grab from a live audio/video source.					
Denial of Service	23-12-2016	4.3	The che_configure function in libavcodec/aacdec_template.c in FFmpeg before 3.2.1 allows remote attackers to cause a denial of service (allocation of huge memory, and being killed by the OS) via a crafted MOV file. **REFERENCE: CVE-2016-9561**	NA	A-FFM-FFMPE-030116/09
Denial of Service	23-12-2016	4.3	The gsm_parse function in libavcodec/gsm_parser.c in FFmpeg before 3.1.5 allows remote attackers to cause a denial of service (assert fault) via a crafted AVI file. **REFERENCE: CVE-2016-8595**	NA	A-FFM-FFMPE-030116/10
Denial of Service	23-12-2016	4.3	The read_gab2_sub function in libavformat/avidec.c in FFmpeg before 3.1.4 allows remote attackers to cause a denial of service (NULL pointer used) via a crafted AVI file. **REFERENCE: CVE-2016-7905**	NA	A-FFM-FFMPE-030116/11
Denial of Service	23-12-2016	4.3	The avi_read_seek function in libavformat/avidec.c in FFmpeg before 3.1.4 allows remote attackers to cause a denial of service (assert fault)	NA	A-FFM-FFMPE-030116/12

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			via a crafted AVI file. **REFERENCE: CVE-2016-7785**		
Denial of Service; Overflow	23-12-2016	4.3	The ff_draw_pc_font function in libavcodec/cga_data.c in FFmpeg before 3.1.4 allows remote attackers to cause a denial of service (buffer overflow) via a crafted AVI file. **REFERENCE: CVE-2016-7562**	NA	A-FFM-FFMPE-030116/13
Gain Information	23-12-2016	4.3	The avi_read_header function in libavformat/avidec.c in FFmpeg before 3.1.4 is vulnerable to memory leak when decoding an AVI file that has a crafted "strh" structure. **REFERENCE: CVE-2016-7555**	NA	A-FFM-FFMPE-030116/14
NA	23-12-2016	6.8	The cavs_idct8_add_c function in libavcodec/cavsdsp.c in FFmpeg before 3.1.4 is vulnerable to reading out-of-bounds memory when decoding with cavs_decode. **REFERENCE: CVE-2016-7502**	NA	A-FFM-FFMPE-030116/15
NA	23-12-2016	6.8	The ff_log2_16bit_c function in libavutil/intmath.h in FFmpeg before 3.1.4 is vulnerable to reading out-of-bounds memory when it decodes a malformed AIFF file. **REFERENCE: CVE-2016-7450**	NA	A-FFM-FFMPE-030116/16
NA	23-12-2016	4.3	The avi_read_nikon function in libavformat/avidec.c in FFmpeg before 3.1.4 is vulnerable to infinite loop when it decodes an AVI file that has a crafted 'nctg' structure. **REFERENCE: CVE-2016-7122**	NA	A-FFM-FFMPE-030116/17
Denial of Service	23-12-2016	4.3	The zlib_refill function in libavformat/swfdec.c in FFmpeg before 3.1.3 allows remote attackers to cause an infinite loop denial of service via a crafted SWF file. **REFERENCE: CVE-2016-6881**	NA	A-FFM-FFMPE-030116/18

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Denial of Service; Execute Code; Overflow; Memory Corruption	23-12-2016	6.8	The raw_decode function in libavcodec/rawdec.c in FFmpeg before 3.1.2 allows remote attackers to cause a denial of service (memory corruption) or execute arbitrary code via a crafted SWF file. **REFERENCE: CVE-2016-6671**	NA	A-FFM-FFMPE-030116/19
Google					
Chrome Google Chrome is a freeware web browser developed by Google.					
Gain Information	17-12-2016	4.3	Google Chrome prior to 54.0.2840.85 for Android incorrectly handled rapid transition into and out of full screen mode, which allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via crafted HTML pages. **REFERENCE: CVE-2016-5187**	https://crbug.com/639702	A-GOO-CHROM-030116/20
Execute Code	17-12-2016	6.8	Devtools in Google Chrome prior to 54.0.2840.59 for Windows, Mac, and Linux; 54.0.2840.85 for Android incorrectly handled objects after a tab crash, which allowed a remote attacker to perform an out of bounds memory read via crafted PDF files. **REFERENCE: CVE-2016-5186**	https://crbug.com/644963	A-GOO-CHROM-030116/21
Cross Site Scripting	17-12-2016	6.8	Blink in Google Chrome prior to 54.0.2840.59 for Windows, Mac, and Linux; 54.0.2840.85 for Android incorrectly allowed reentrance of FrameView::updateLifecyclePhasesInternal(), which allowed a remote attacker to perform an out of bounds memory read via crafted HTML pages. **REFERENCE: CVE-2016-5185**	https://crbug.com/621360	A-GOO-CHROM-030116/22
Cross Site Scripting	17-12-2016	6.8	PDFium in Google Chrome prior to 54.0.2840.59 for	https://crbug.com/63065	A-GOO-CHROM-

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			Windows, Mac, and Linux; 54.0.2840.85 for Android incorrectly handled object lifecycles in CFFL_FormFillter::KillFocusForAnnot, which allowed a remote attacker to potentially exploit heap corruption via crafted PDF files. **REFERENCE: CVE-2016-5184**	4	030116/23
Execute Code; Overflow	17-12-2016	6.8	A heap use after free in PDFium in Google Chrome prior to 54.0.2840.59 for Windows, Mac, and Linux; 54.0.2840.85 for Android allows a remote attacker to potentially exploit heap corruption via crafted PDF files. **REFERENCE: CVE-2016-5183**	https://chromereleases.googleblog.com/2016/10/stable-channel-update-for-desktop.html	A-GOO-CHROM-030116/24
Overflow	17-12-2016	6.8	Blink in Google Chrome prior to 54.0.2840.59 for Windows, Mac, and Linux; 54.0.2840.85 for Android had insufficient validation in bitmap handling, which allowed a remote attacker to potentially exploit heap corruption via crafted HTML pages. **REFERENCE: CVE-2016-5182**	https://chromereleases.googleblog.com/2016/10/stable-channel-update-for-desktop.html	A-GOO-CHROM-030116/25
Cross Site Scripting	17-12-2016	4.3	Blink in Google Chrome prior to 54.0.2840.59 for Windows, Mac, and Linux; 54.0.2840.85 for Android permitted execution of v8 microtasks while the DOM was in an inconsistent state, which allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via crafted HTML pages. **REFERENCE: CVE-2016-5181**	https://crbug.com/645211	A-GOO-CHROM-030116/26
Bypass	17-12-2016	4.3	Google Chrome prior to 54.0 for iOS had insufficient validation of URLs for	https://crbug.com/639658	A-GOO-CHROM-030116/27

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			windows open by DOM, which allowed a remote attacker to bypass restrictions on navigation to certain URL schemes via crafted HTML pages. **REFERENCE: CVE-2016-5193**		
Bypass	17-12-2016	4.3	Blink in Google Chrome prior to 54.0.2840.59 for Windows missed a CORS check on redirect in TextTrackLoader, which allowed a remote attacker to bypass cross-origin restrictions via crafted HTML pages. **REFERENCE: CVE-2016-5192**	https://crbug.com/633885	A-GOO-CHROM-030116/28
Cross Site Scripting	17-12-2016	4.3	Bookmark handling in Google Chrome prior to 54.0.2840.59 for Windows, Mac, and Linux; 54.0.2840.85 for Android had insufficient validation of supplied data, which allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via crafted HTML pages, as demonstrated by an interpretation conflict between userinfo and scheme in an http://javascript:payload@example.com URL. **REFERENCE: CVE-2016-5191**	https://crbug.com/639126	A-GOO-CHROM-030116/29
NA	17-12-2016	6.8	Google Chrome prior to 54.0.2840.59 for Windows, Mac, and Linux; 54.0.2840.85 for Android incorrectly handled object lifecycles during shutdown, which allowed a remote attacker to perform an out of bounds memory read via crafted HTML pages. **REFERENCE: CVE-2016-5190**	https://crbug.com/642067	A-GOO-CHROM-030116/30
NA	17-12-2016	4.3	Google Chrome prior to 54.0.2840.59 for Windows, Mac, and Linux; 54.0.2840.85	https://crbug.com/646278	A-GOO-CHROM-030116/31

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			for Android permitted navigation to blob URLs with non-canonical origins, which allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via crafted HTML pages. **REFERENCE: CVE-2016-5189**		
NA	17-12-2016	4.3	Multiple issues in Blink in Google Chrome prior to 54.0.2840.59 for Windows, Mac, and Linux allow a remote attacker to spoof various parts of browser UI via crafted HTML pages. **REFERENCE: CVE-2016-5188**	https://crbug.com/565760	A-GOO-CHROM-030116/32
NA	17-12-2016	4.3	Google Chrome prior to 54.0.2840.85 for Android incorrectly handled rapid transition into and out of full screen mode, which allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via crafted HTML pages. **REFERENCE: CVE-2016-5187**	https://crbug.com/639702	A-GOO-CHROM-030116/33
NA	17-12-2016	6.8	Devtools in Google Chrome prior to 54.0.2840.59 for Windows, Mac, and Linux; 54.0.2840.85 for Android incorrectly handled objects after a tab crash, which allowed a remote attacker to perform an out of bounds memory read via crafted PDF files. **REFERENCE: CVE-2016-5186**	https://crbug.com/644963	A-GOO-CHROM-030116/34
NA	17-12-2016	6.8	Blink in Google Chrome prior to 54.0.2840.59 for Windows, Mac, and Linux; 54.0.2840.85 for Android incorrectly allowed reentrance of FrameView::updateLifecyclePhasesInternal(), which allowed a remote attacker to perform an out of bounds memory read	https://crbug.com/621360	A-GOO-CHROM-030116/35

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			via crafted HTML pages. **REFERENCE: CVE-2016-5185**		
NA	17-12-2016	6.8	PDFium in Google Chrome prior to 54.0.2840.59 for Windows, Mac, and Linux; 54.0.2840.85 for Android incorrectly handled object lifecycles in CFFL_FormFillter::KillFocusForAnnot, which allowed a remote attacker to potentially exploit heap corruption via crafted PDF files. **REFERENCE: CVE-2016-5184**	https://crbug.com/630654	A-GOO-CHROM-030116/36
NA	17-12-2016	6.8	A heap use after free in PDFium in Google Chrome prior to 54.0.2840.59 for Windows, Mac, and Linux; 54.0.2840.85 for Android allows a remote attacker to potentially exploit heap corruption via crafted PDF files. **REFERENCE: CVE-2016-5183**	https://chromereleases.googleblog.com/2016/10/stable-channel-update-for-desktop.html	A-GOO-CHROM-030116/37
Overflow	17-12-2016	6.8	Blink in Google Chrome prior to 54.0.2840.59 for Windows, Mac, and Linux; 54.0.2840.85 for Android had insufficient validation in bitmap handling, which allowed a remote attacker to potentially exploit heap corruption via crafted HTML pages. **REFERENCE: CVE-2016-5182**	https://chromereleases.googleblog.com/2016/10/stable-channel-update-for-desktop.html	A-GOO-CHROM-030116/38
Cross Site Scripting	17-12-2016	4.3	Blink in Google Chrome prior to 54.0.2840.59 for Windows, Mac, and Linux; 54.0.2840.85 for Android permitted execution of v8 microtasks while the DOM was in an inconsistent state, which allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via crafted HTML pages.	https://crbug.com/645211	A-GOO-CHROM-030116/39

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			REFERENCE: CVE-2016-5181		
Horde					
Groupware Horde Groupware is a free, enterprise ready, browser based collaboration suite.					
Cross Site Scripting	20-12-2016	4.3	Cross-site scripting (XSS) vulnerability in the Horde Text Filter API in Horde Groupware and Horde Groupware Webmail Edition before 5.2.16 allows remote attackers to inject arbitrary web script or HTML via crafted data:text/html content in a form (1) action or (2) xlink attribute. **REFERENCE: CVE-2016-5303**	NA	A-HOR-GROUP-030116/40
Image-info Project					
Image-info For Perl NA					
Denial of Service	22-12-2016	5.8	perl-Image-Info: When parsing an SVG file, external entity expansion (XXE) was not disabled. An attacker could craft an SVG file which, when processed by an application using perl-Image-Info, could cause denial of service or, potentially, information disclosure. **REFERENCE: CVE-2016-9181**	NA	A-IMA-IMAGE-030116/41
Imagemagick					
Imagemagick ImageMagick is a software suite to create, edit, compose, or convert bitmap images.					
Execute Code	23-12-2016	6.8	An exploitable out of bounds write exists in the handling of compressed TIFF images in ImageMagicks's convert utility. A crafted TIFF document can lead to an out of bounds write which in particular circumstances could be leveraged into remote code execution. The vulnerability can be triggered through any	NA	A-IMA-IMAGE-030116/42

			user controlled TIFF that is handled by this functionality. **REFERENCE: CVE-2016-8707**		
Joomla					
Joomla! Joomla! is the mobile-ready and user-friendly way to build your website.					
NA	16-12-2016	5	An issue was discovered in components/com_users/models/registration.php in Joomla! before 3.6.5. Incorrect filtering of registration form data stored to the session on a validation error enables a user to gain access to a registered user's account and reset the user's group mappings, username, and password, as demonstrated by submitting a form that targets the `registration.register` task. **REFERENCE: CVE-2016-9838**	https://www.joomla.org/announcements/release-news/5693-joomla-3-6-5-released.html	A-JOO-JOOML-030116/43
NA	16-12-2016	5	An issue was discovered in templates/beez3/html/com_content/article/default.php in Joomla! before 3.6.5. Inadequate permissions checks in the Beez3 layout override of the com_content article view allow users to view articles that should not be publicly accessible, as demonstrated by an index.php?option=com_content&view=article&id=1&template=beez3 request. **REFERENCE: CVE-2016-9837**	https://www.joomla.org/announcements/release-news/5693-joomla-3-6-5-released.html	A-JOO-JOOML-030116/44
KDE					
Kmail KMail is the email component of Kontact, the integrated personal information manager from KDE.					
Execute Code	23-12-2016	7.5	KMail since version 5.3.0 used a QWebEngine based viewer that had JavaScript enabled. HTML Mail contents were not sanitized for JavaScript and included code was executed.	NA	A-KDE-KMAIL-030116/45

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			REFERENCE: CVE-2016-7968		
NA	23-12-2016	5.8	KMail since version 5.3.0 used a QWebEngine based viewer that had JavaScript enabled. Since the generated html is executed in the local file security context by default access to remote and local URLs was enabled. **REFERENCE: CVE-2016-7967**	NA	A-KDE-KMAIL-030116/46
Lynx					
Lynx Lynx is a highly configurable text-based web browser for use on cursor-addressable character cell terminals.					
NA	22-12-2016	5	lynx: It was found that Lynx doesn't parse the authority component of the URL correctly when the host name part ends with '?', and could instead be tricked into connecting to a different host. **REFERENCE: CVE-2016-9179**	NA	A-LYN-LYNX-030116/47
Microsoft					
.net Framework .NET Framework (pronounced dot net) is a software framework developed by Microsoft that runs primarily on Microsoft Windows.					
Bypass; Gain Information	20-12-2016	5	The Data Provider for SQL Server in Microsoft .NET Framework 4.6.2 mishandles a developer-supplied key, which allows remote attackers to bypass the Always Encrypted protection mechanism and obtain sensitive cleartext information by leveraging key guessability, aka ".NET Information Disclosure Vulnerability." **REFERENCE: CVE-2016-7270**	NA	A-MIC-.NET -030116/48
Auto Updater For Mac Download, Install or Update Microsoft AutoUpdate (Mac) - Provides latest MS Office updates to customers - MacUpdate.					
Gain Privileges	20-12-2016	4.6	Untrusted search path vulnerability in Microsoft Auto	NA	A-MIC-AUTO -

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			Updater for Mac allows local users to gain privileges via a Trojan horse executable file, aka "Microsoft (MAU) Office Elevation of Privilege Vulnerability." **REFERENCE: CVE-2016-7300**		030116/49
Edge Experience Microsoft Edge, the all new browser for having a better web experience.					
Denial of Service; Execute Code; Overflow; Memory Corruption	20-12-2016	7.6	The scripting engines in Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability," a different vulnerability than CVE-2016-7286, CVE-2016-7288, and CVE-2016-7296. **REFERENCE: CVE-2016-7297**	NA	A-MIC-EDGE-030116/50
Denial of Service; Execute Code; Overflow; Memory Corruption	20-12-2016	7.6	The scripting engines in Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability," a different vulnerability than CVE-2016-7286, CVE-2016-7288, and CVE-2016-7297. **REFERENCE: CVE-2016-7296**	NA	A-MIC-EDGE-030116/51
Denial of Service; Execute Code; Overflow; Memory Corruption	20-12-2016	7.6	The scripting engines in Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability," a different vulnerability than CVE-2016-7286, CVE-2016-7296, and CVE-2016-7297. **REFERENCE: CVE-2016-7288**	NA	A-MIC-EDGE-030116/52

Denial of Service; Execute Code; Overflow; Memory Corruption	20-12-2016	7.6	The scripting engines in Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability," a different vulnerability than CVE-2016-7288, CVE-2016-7296, and CVE-2016-7297. **REFERENCE: CVE-2016-7286**	NA	A-MIC-EDGE-030116/53
Cross Site Scripting	20-12-2016	4.3	Cross-site scripting (XSS) vulnerability in Microsoft Edge allows remote attackers to inject arbitrary web script or HTML via unspecified vectors, aka "Microsoft Edge Information Disclosure Vulnerability," a different vulnerability than CVE-2016-7206. **REFERENCE: CVE-2016-7280**	NA	A-MIC-EDGE-030116/54
Cross Site Scripting	20-12-2016	4.3	Cross-site scripting (XSS) vulnerability in Microsoft Edge allows remote attackers to inject arbitrary web script or HTML via unspecified vectors, aka "Microsoft Edge Information Disclosure Vulnerability," a different vulnerability than CVE-2016-7280. **REFERENCE: CVE-2016-7206**	NA	A-MIC-EDGE-030116/55
Denial of Service; Execute Code; Overflow; Memory Corruption	20-12-2016	7.6	Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Edge Memory Corruption Vulnerability." **REFERENCE: CVE-2016-7181**	NA	A-MIC-EDGE-030116/56

Edge;Internet Explorer

Experience Microsoft Edge, the all new browser for having a better web experience; Internet Explorer is a discontinued series of graphical web browsers developed by Microsoft and included as part of the

Microsoft Windows line of operating systems, starting in 1995.					
Denial of Service; Execute Code; Overflow; Memory Corruption	20-12-2016	7.6	The scripting engines in Microsoft Internet Explorer 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability." **REFERENCE: CVE-2016-7287**	NA	A-MIC-EDGE;-030116/57
Cross Site Scripting	20-12-2016	4.3	Cross-site scripting (XSS) vulnerability in Microsoft Internet Explorer 9 through 11 and Microsoft Edge allows remote attackers to inject arbitrary web script or HTML via unspecified vectors, aka "Microsoft Browser Information Disclosure Vulnerability." **REFERENCE: CVE-2016-7282**	NA	A-MIC-EDGE;-030116/58
Bypass	20-12-2016	2.6	The Web Workers implementation in Microsoft Internet Explorer 10 and 11 and Microsoft Edge allows remote attackers to bypass the Same Origin Policy via unspecified vectors, aka "Microsoft Browser Security Feature Bypass Vulnerability." **REFERENCE: CVE-2016-7281**	NA	A-MIC-EDGE;-030116/59
Denial of Service; Execute Code; Overflow; Memory Corruption	20-12-2016	7.6	Microsoft Internet Explorer 9 through 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Corruption Vulnerability." **REFERENCE: CVE-2016-7279**	NA	A-MIC-EDGE;-030116/60
Excel Microsoft Excel is a spreadsheet developed by Microsoft for Windows, macOS, Android and iOS.					

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Execute Code; Bypass	20-12-2016	4.3	Microsoft Excel 2010 SP2, 2013 SP1, 2013 RT SP1, and 2016 misparses file formats, which makes it easier for remote attackers to execute arbitrary code via a crafted document, aka "Microsoft Office Security Feature Bypass Vulnerability." **REFERENCE: CVE-2016-7267**	NA	A-MIC-EXCEL-030116/61
Excel For Mac Microsoft Excel better than ever for Mac, and much more programs.					
Denial of Service; Execute Code; Overflow; Memory Corruption	20-12-2016	9.3	Microsoft Excel for Mac 2011 and Excel 2016 for Mac allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted document, aka "Microsoft Office Memory Corruption Vulnerability." **REFERENCE: CVE-2016-7263**	NA	A-MIC-EXCEL-030116/62
Excel;Excel For Mac;Excel Viewer;Office Compatibility Pack Microsoft Excel is a spreadsheet developed by Microsoft for Windows, macOS, Android and iOS; Microsoft Excel better than ever for Mac, and much more programs; The Free Excel Viewer allows a user to open, view and print MS Excel files without installing Microsoft Excel on his or her system; Microsoft Office Compatibility Pack makes files created with Office 2007 and later work seamlessly on earlier versions of Office.					
Execute Code; Bypass	20-12-2016	6.8	Microsoft Excel 2007 SP3, Excel 2010 SP2, Excel 2013 SP1, Excel 2013 RT SP1, Excel 2016, Office Compatibility Pack SP3, Excel Viewer, and Excel 2016 for Mac mishandle a registry check, which allows user-assisted remote attackers to execute arbitrary commands via crafted embedded content in a document, aka "Microsoft Office Security Feature Bypass Vulnerability." **REFERENCE: CVE-2016-7266**	NA	A-MIC-EXCEL-030116/63
Denial of Service; Gain	20-12-2016	5.8	Microsoft Excel 2007 SP3, Office Compatibility Pack SP3,	NA	A-MIC-EXCEL-

Information			Excel Viewer, Excel for Mac 2011, and Excel 2016 for Mac allow remote attackers to obtain sensitive information from process memory or cause a denial of service (out-of-bounds read) via a crafted document, aka "Microsoft Office Information Disclosure Vulnerability." **REFERENCE: CVE-2016-7264**		030116/64
Execute Code; Bypass	20-12-2016	6.8	Microsoft Excel 2007 SP3, Excel 2010 SP2, Excel 2013 SP1, Excel 2013 RT SP1, Excel 2016, Office Compatibility Pack SP3, and Excel Viewer allow user-assisted remote attackers to execute arbitrary commands via a crafted cell that is mishandled upon a click, aka "Microsoft Office Security Feature Bypass Vulnerability." **REFERENCE: CVE-2016-7262**	NA	A-MIC-EXCEL-030116/65
Excel;Excel Viewer;Office Compatibility Pack;Sharepoint Server Microsoft Excel is a spreadsheet developed by Microsoft for Windows, macOS, Android and iOS; The Free Excel Viewer allows a user to open, view and print MS Excel files without installing Microsoft Excel on his or her system; Microsoft Office SharePoint Server (MOSS) is the full version of a portal-based platform for collaboratively creating, managing and sharing documents and Web services.					
Denial of Service; Gain Information	20-12-2016	5.8	Microsoft Excel 2007 SP3, Excel 2010 SP2, Excel 2013 SP1, Excel 2013 RT SP1, Excel 2016, Office Compatibility Pack SP3, Excel Viewer, Excel Services on SharePoint Server 2007 SP3, and Excel Services on SharePoint Server 2010 SP2 allow remote attackers to obtain sensitive information from process memory or cause a denial of service (out-of-bounds read) via a crafted document, aka "Microsoft Office Information Disclosure Vulnerability."	NA	A-MIC-EXCEL-030116/66

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			REFERENCE: CVE-2016-7265		
Internet Explorer Internet Explorer is a discontinued series of graphical web browsers developed by Microsoft and included as part of the Microsoft Windows line of operating systems, starting in 1995.					
Gain Information	20-12-2016	4.3	Microsoft Internet Explorer 10 and 11 allows remote attackers to obtain sensitive information from process memory via a crafted web site, aka "Internet Explorer Information Disclosure Vulnerability." **REFERENCE: CVE-2016-7284**	NA	A-MIC-INTER-030116/67
Denial of Service; Execute Code; Overflow; Memory Corruption	20-12-2016	9.3	Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability." **REFERENCE: CVE-2016-7283**	NA	A-MIC-INTER-030116/68
Gain Information	20-12-2016	2.6	Microsoft Internet Explorer 9 through 11 allows remote attackers to obtain sensitive information from process memory via a crafted web site, aka "Windows Hyperlink Object Library Information Disclosure Vulnerability." **REFERENCE: CVE-2016-7278**	NA	A-MIC-INTER-030116/69
Office Microsoft Office is an office suite of applications, servers, and services developed by Microsoft.					
Denial of Service; Execute Code; Overflow; Memory Corruption	20-12-2016	9.3	Microsoft Office 2016 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted document, aka "Microsoft Office Memory Corruption Vulnerability." **REFERENCE: CVE-2016-7277**	NA	A-MIC-OFFIC-030116/70
Gain Privileges	20-12-2016	7.2	Microsoft Office 2010 SP2, 2013 SP1, 2013 RT SP1, and 2016 mishandles library	NA	A-MIC-OFFIC-030116/71

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			loading, which allows local users to gain privileges via a crafted application, aka "Microsoft Office OLE DLL Side Loading Vulnerability." **REFERENCE: CVE-2016-7275**		
Office;Office Compatibility Pack;Office Web Apps;Sharepoint Server;Word;Word Automation Services;Word For Mac Microsoft Office is an office suite of applications, servers, and services developed by Microsoft; Microsoft Office Compatibility Pack makes files created with Office 2007 and later work seamlessly on earlier versions of Office; Office Online (previously Office Web Apps) is an online office suite offered by Microsoft, which allows users to create and edit files using lightweight, web browser-based versions of Microsoft Office applications: Word, Excel, PowerPoint and OneNote; Microsoft Office SharePoint Server (MOSS) is the full version of a portal-based platform for collaboratively creating, managing and sharing documents and Web services; Microsoft Word is a word processor developed by Microsoft; Word Automation Services is a new SharePoint Server 2010 technology that enables unattended, server-side conversion of documents that are supported by Microsoft Word; Made with Mac in mind, Office 2016 for Mac gives you access to your favorite Office applications - anywhere, anytime and with anyone- includes new versions of Word, Excel, PowerPoint, Outlook, and OneNote.					
Denial of Service; Gain Information	20-12-2016	5.8	Microsoft Word 2007 SP3, Office 2010 SP2, Word 2010 SP2, Office Compatibility Pack SP3, Word for Mac 2011, Word Automation Services on SharePoint Server 2010 SP2, and Office Web Apps 2010 SP2 allow remote attackers to obtain sensitive information from process memory or cause a denial of service (out-of-bounds read) via a crafted document, aka "Microsoft Office Information Disclosure Vulnerability," a different vulnerability than CVE-2016-7290. **REFERENCE: CVE-2016-7291**	NA	A-MIC-OFFIC-030116/72
Denial of Service; Gain Information	20-12-2016	5.8	Microsoft Word 2007 SP3, Office 2010 SP2, Word 2010 SP2, Office Compatibility Pack SP3, Word for Mac 2011, Word Automation Services on SharePoint Server 2010 SP2, and Office Web Apps 2010 SP2 allow remote attackers to	NA	A-MIC-OFFIC-030116/73

			obtain sensitive information from process memory or cause a denial of service (out-of-bounds read) via a crafted document, aka "Microsoft Office Information Disclosure Vulnerability," a different vulnerability than CVE-2016-7291. **REFERENCE: CVE-2016-7290**		
Denial of Service; Gain Information	20-12-2016	5.8	Microsoft Word 2007 SP3, Office 2010 SP2, Word 2010 SP2, Office Compatibility Pack SP3, Word Viewer, Word for Mac 2011, Word Automation Services on SharePoint Server 2010 SP2, and Office Web Apps 2010 SP2 allow remote attackers to obtain sensitive information from process memory or cause a denial of service (out-of-bounds read) via a crafted document, aka "Microsoft Office Information Disclosure Vulnerability." **REFERENCE: CVE-2016-7268**	NA	A-MIC-OFFIC-030116/74
Office;Office For Mac Microsoft Office is an office suite of applications, servers, and services developed by Microsoft; Office 2016 for Mac is now available with an Office 365 subscription and as a one-time purchase.					
Denial of Service; Gain Information	20-12-2016	5.8	Microsoft Office 2007 SP3, Office 2010 SP2, Office 2013 SP1, Office for Mac 2011, and Office 2016 for Mac allow remote attackers to obtain sensitive information from process memory or cause a denial of service (out-of-bounds read) via a crafted document, aka "Microsoft Office Information Disclosure Vulnerability." **REFERENCE: CVE-2016-7276**	NA	A-MIC-OFFIC-030116/75
Office;Word Viewer Microsoft Office is an office suite of applications, servers, and services developed by Microsoft; Microsoft Word Viewer is a freeware program for Microsoft Windows that can display and print					

Microsoft Word documents.					
Denial of Service; Execute Code; Overflow; Memory Corruption	20-12-2016	9.3	Microsoft Office 2007 SP3, Office 2010 SP2, Word Viewer, Office for Mac 2011, and Office 2016 for Mac allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted document, aka "Microsoft Office Memory Corruption Vulnerability." **REFERENCE: CVE-2016-7298**	NA	A-MIC-OFFIC-030116/76
Publisher Microsoft Publisher is an entry-level desktop publishing application from Microsoft.					
Denial of Service; Execute Code; Overflow; Memory Corruption	20-12-2016	9.3	Microsoft Publisher 2010 SP2 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted document, aka "Microsoft Office Memory Corruption Vulnerability." **REFERENCE: CVE-2016-7289**	NA	A-MIC-PUBLI-030116/77
Netapp					
Snap Creator Framework OS-independent Snap Creator Framework integrates NetApp data protection with a broad range of third-party applications.					
Gain Information	21-12-2016	5	NetApp Snap Creator Framework before 4.3.1 discloses sensitive information which could be viewed by an unauthorized user. **REFERENCE: CVE-2016-7172**	NA	A-NET-SNAP - 030116/78
Nvidia					
Geforce Experience Redesigned from the ground up to be fast and lightweight, the new GeForce Experience keeps your gaming rig updated and running better than ever before.					
Directory Traversal	16-12-2016	5	NVIDIA GeForce Experience 3.x before GFE 3.1.0.52 contains a vulnerability in NVIDIA Web Helper.exe where a local web API endpoint, /VisualOPS/v.1.0./, lacks proper access control and	http://nvidia.custhelp.com/app/answers/detail/a_id/4279	A-NVI-GEFOR-030116/79

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			parameter validation, allowing for information disclosure via a directory traversal attack. **REFERENCE: CVE-2016-8827**		
Gpu Driver NVIDIA GPUs drive a visually stunning, premium experience on desktop and notebook PCs.					
Denial of Service	16-12-2016	4.9	All versions of NVIDIA GPU Display Driver contain a vulnerability in the kernel mode layer (nvlddmkm.sys for Windows or nvidia.ko for Linux) where a user can cause a GPU interrupt storm, leading to a denial of service. **REFERENCE: CVE-2016-8826**	http://nvidia.custhelp.com/app/answers/detail/a_id/4278	A-NVI-GPUD-030116/80
Denial of Service; Overflow	16-12-2016	7.2	All versions of NVIDIA Windows GPU Display Driver contain a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgDdiEscape where the size of an input buffer is not validated, leading to denial of service or potential escalation of privileges. **REFERENCE: CVE-2016-8825**	http://nvidia.custhelp.com/app/answers/detail/a_id/4278	A-NVI-GPUD-030116/81
NA	16-12-2016	7.2	All versions of NVIDIA Windows GPU Display Driver contain a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgDdiEscape where improper access controls allow a regular user to write a part of the registry intended for privileged users only, leading to escalation of privileges. **REFERENCE: CVE-2016-8824**	http://nvidia.custhelp.com/app/answers/detail/a_id/4278	A-NVI-GPUD-030116/82
Denial of Service; Overflow	16-12-2016	7.2	All versions of NVIDIA Windows GPU Display Driver contain a vulnerability in the kernel mode layer handler for DxgDdiEscape where the size of an input buffer is not validated leading to a denial of	http://nvidia.custhelp.com/app/answers/detail/a_id/4278	A-NVI-GPUD-030116/83

			service or possible escalation of privileges **REFERENCE: CVE-2016-8823**		
Denial of Service	16-12-2016	7.2	All versions of NVIDIA Windows GPU Display Driver contain a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgDdiEscape ID 0x600000E, 0x600000F, and 0x6000010 where a value passed from a user to the driver is used without validation as the index to an internal array, leading to denial of service or potential escalation of privileges. **REFERENCE: CVE-2016-8822**	http://nvidia.custhelp.com/app/answers/detail/a_id/4278	A-NVI-GPUD-030116/84
NA	16-12-2016	7.2	All versions of NVIDIA Windows GPU Display Driver contain a vulnerability in the kernel mode layer handler for DxgDdiEscape where improper access controls may allow a user to access arbitrary physical memory, leading to an escalation of privileges. **REFERENCE: CVE-2016-8821**	http://nvidia.custhelp.com/app/answers/detail/a_id/4278	A-NVI-GPUD-030116/85
Denial of Service	16-12-2016	5.6	All versions of NVIDIA Windows GPU Display Driver contain a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgDdiEscape where a check on a function return value is missing, potentially allowing an uninitialized value to be used as the source of a strcpy() call, leading to denial of service or information disclosure. **REFERENCE: CVE-2016-8820**	http://nvidia.custhelp.com/app/answers/detail/a_id/4257	A-NVI-GPUD-030116/86
Denial of Service	16-12-2016	7.2	All versions of NVIDIA Windows GPU Display Driver contain a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for	http://nvidia.custhelp.com/app/answers/detail/a_id/4257	A-NVI-GPUD-030116/87

			DxgkDdiEscape where a handle to a kernel object may be returned to the user, leading to possible denial of service or escalation of privileges. **REFERENCE: CVE-2016-8819**		
Denial of Service	16-12-2016	7.2	All versions of NVIDIA Windows GPU Display contain a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgDdiEscape where a pointer passed from a user to the driver is used without validation, leading to denial of service or potential escalation of privileges. **REFERENCE: CVE-2016-8818**	http://nvidia.custhelp.com/app/answers/detail/a_id/4257	A-NVI-GPUD-030116/88
Denial of Service; Overflow	16-12-2016	7.2	All versions of NVIDIA Windows GPU Display Driver contain a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgDdiEscape where a value passed from a user to the driver is used without validation as the size input to memcpy(), causing a buffer overflow, leading to denial of service or potential escalation of privileges. **REFERENCE: CVE-2016-8817**	http://nvidia.custhelp.com/app/answers/detail/a_id/4257	A-NVI-GPUD-030116/89
Denial of Service	16-12-2016	7.2	All versions of NVIDIA Windows GPU Display Driver contain a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgDdiEscape where a value passed from a user to the driver is used without validation as the index to an array, leading to denial of service or potential escalation of privileges. **REFERENCE: CVE-2016-8816**	http://nvidia.custhelp.com/app/answers/detail/a_id/4257	A-NVI-GPUD-030116/90

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Denial of Service	16-12-2016	7.2	All versions of NVIDIA Windows GPU Display Driver contain a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgDdiEscape where a value passed from a user to the driver is used without validation as the index to an array, leading to denial of service or potential escalation of privileges. **REFERENCE: CVE-2016-8815**	http://nvidia.custhelp.com/app/answers/detail/a_id/4257	A-NVI-GPUD-030116/91
Denial of Service	16-12-2016	7.2	All versions of NVIDIA Windows GPU Display Driver contain a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgDdiEscape where multiple pointers are used without checking for NULL, leading to denial of service or potential escalation of privileges. **REFERENCE: CVE-2016-8814**	http://nvidia.custhelp.com/app/answers/detail/a_id/4257	A-NVI-GPUD-030116/92
Denial of Service	16-12-2016	7.2	All versions of NVIDIA Windows GPU Display Driver contain a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgDdiEscape where multiple pointers are used without checking for NULL, leading to denial of service or potential escalation of privileges. **REFERENCE: CVE-2016-8813**	http://nvidia.custhelp.com/app/answers/detail/a_id/4257	A-NVI-GPUD-030116/93
Openjpeg					
Openjpeg OpenJPEG is an open-source JPEG 2000 codec written in C language.					
Execute Code; Overflow	22-12-2016	6.8	openjpeg: A heap-based buffer overflow flaw was found in the patch for CVE-2013-6045. A crafted j2k image could cause the application to crash, or potentially execute arbitrary code.	NA	A-OPE-OPENJ-030116/94

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			REFERENCE: CVE-2016-9675		
Pivotal Software					
Cloud Foundry Elastic Runtime; Cloud Foundry Ops Manager Cloud Foundry is an open platform as a service, providing a choice of clouds, developer frameworks, and application services.					
NA	16-12-2016	5.8	An open redirect vulnerability has been detected with some Pivotal Cloud Foundry Elastic Runtime components. Users of affected versions should apply the following mitigation: Upgrade PCF Elastic Runtime 1.8.x versions to 1.8.12 or later. Upgrade PCF Ops Manager 1.7.x versions to 1.7.18 or later and 1.8.x versions to 1.8.10 or later. **REFERENCE: CVE-2016-6657**	https://pivotal.io/security/Reference: CVE-2016-6657	A-PIV-CLOUD-030116/95
Cloud Foundry;Cloud Foundry Uaa; Cloud Foundry Uaa Bosh Cloud Foundry is an open platform as a service, providing a choice of clouds, developer frameworks, and application services; CloudFoundry UAA stands for User Account and Authentication Server.					
Gain Privileges	23-12-2016	2.6	Cloud Foundry before 248; UAA 2.x before 2.7.4.12, 3.x before 3.6.5, and 3.7.x through 3.9.x before 3.9.3; and UAA bosh release (aka uaa-release) before 13.9 for UAA 3.6.5 and before 24 for UAA 3.9.3 allow attackers to gain privileges by accessing UAA logs and subsequently running a specially crafted application that interacts with a configured SAML provider. **REFERENCE: CVE-2016-6659**	https://www.cloudfoundry.org/Reference: CVE-2016-6659/	A-PIV-CLOUD-030116/96
Greenplum Greenplum Database is an advanced, fully featured, open source data warehouse.					
NA	16-12-2016	6.5	An issue was discovered in Pivotal Greenplum before 4.3.10.0. Creation of external tables using GPHDFS protocol has a vulnerability whereby arbitrary commands can be injected into the system. In order to exploit this	https://pivotal.io/security/Reference: CVE-2016-6656	A-PIV-GREEN-030116/97

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			vulnerability the user must have superuser 'gpadmin' access to the system or have been granted GPHDFS protocol permissions in order to create a GPHDFS external table. **REFERENCE: CVE-2016-6656**		
Rabbitmq RabbitMQ is open source message broker software that implements the Advanced Message Queuing Protocol (AMQP).					
NA	29-12-2016	7.5	An issue was discovered in Pivotal RabbitMQ 3.x before 3.5.8 and 3.6.x before 3.6.6 and RabbitMQ for PCF 1.5.x before 1.5.20, 1.6.x before 1.6.12, and 1.7.x before 1.7.7. MQTT (MQ Telemetry Transport) connection authentication with a username/password pair succeeds if an existing username is provided but the password is omitted from the connection request. Connections that use TLS with a client-provided certificate are not affected. **REFERENCE: CVE-2016-9877**	https://pivotal.io/security/Reference: CVE-2016-9877	A-PIV-RABBI-030116/98
Python-openxml					
Python python-docx is a Python library for creating and updating Microsoft Word (.docx) files.					
NA	21-12-2016	6.8	python-docx before 0.8.6 allows context-dependent attackers to conduct XML External Entity (XXE) attacks via a crafted document. **REFERENCE: CVE-2016-5851**	NA	A-PYT-PYTHO-030116/99
Qemu					
Qemu QEMU is a generic and open source machine emulator and virtualizer.					
Bypass; Gain Information	29-12-2016	2.1	QEMU (aka Quick Emulator) built with the USB EHCI emulation support is vulnerable to a null pointer dereference flaw. It could occur when an application	https://bugzilla.redhat.com/show_bug.cgi?id=1301643	A-QEM-QEMU-030116/100

			attempts to write to EHCI capabilities registers. A privileged user inside quest could use this flaw to crash the QEMU process instance resulting in DoS. **REFERENCE: CVE-2016-2198**		
Bypass	29-12-2016	2.1	QEMU (aka Quick Emulator) built with an IDE AHCI emulation support is vulnerable to a null pointer dereference flaw. It occurs while unmapping the Frame Information Structure (FIS) and Command List Block (CLB) entries. A privileged user inside guest could use this flaw to crash the QEMU process instance resulting in DoS. **REFERENCE: CVE-2016-2197**	https://bugzilla.redhat.com/show_bug.cgi?id=1302057	A-QEM-QEMU-030116/101
Cross Site Scripting	29-12-2016	2.1	QEMU (aka Quick Emulator) built with the e1000 NIC emulation support is vulnerable to an infinite loop issue. It could occur while processing data via transmit or receive descriptors, provided the initial receive/transmit descriptor head (TDH/RDH) is set outside the allocated descriptor buffer. A privileged user inside guest could use this flaw to crash the QEMU instance resulting in DoS. **REFERENCE: CVE-2016-1981**	https://bugzilla.redhat.com/show_bug.cgi?id=1298570	A-QEM-QEMU-030116/102
Bypass	29-12-2016	2.1	QEMU (aka Quick Emulator) built with the TPR optimization for 32-bit Windows guests support is vulnerable to a null pointer dereference flaw. It occurs while doing I/O port write operations via hmp interface. In that, 'current_cpu' remains null, which leads to the null	https://bugzilla.redhat.com/show_bug.cgi?id=1283934	A-QEM-QEMU-030116/103

			pointer dereference. A user or process could use this flaw to crash the QEMU instance, resulting in DoS issue. **REFERENCE: CVE-2016-1922**		
Denial of Service	29-12-2016	2.1	The cpu_physical_memory_write_rom_internal function in exec.c in QEMU (aka Quick Emulator) does not properly skip MMIO regions, which allows local privileged guest users to cause a denial of service (guest crash) via unspecified vectors. **CVE-2015-8818** https://bugzilla.redhat.com/show_bug.cgi?id=1300771	NA	A-QEM-QEMU-030116/104
Overflow	29-12-2016	4.9	QEMU (aka Quick Emulator) built with the Virtio GPU Device emulator support is vulnerable to a memory leakage issue. It could occur while updating the cursor data in update_cursor_data_virgl. A guest user/process could use this flaw to leak host memory bytes, resulting in DoS for a host. **REFERENCE: CVE-2016-9846**	NA	A-QEM-QEMU-030116/105
Gain Information	29-12-2016	2.1	QEMU (aka Quick Emulator) built with the Virtio GPU Device emulator support is vulnerable to an information leakage issue. It could occur while processing 'VIRTIO_GPU_CMD_GET_CAPSET_INFO' command. A guest user/process could use this flaw to leak contents of the host memory bytes. **REFERENCE: CVE-2016-9845**	NA	A-QEM-QEMU-030116/106
NA	29-12-2016	2.1	QEMU (aka Quick Emulator) built with the ColdFire Fast Ethernet Controller emulator support is vulnerable to an	https://bugzilla.redhat.com/show_bug.cgi?id=14008	A-QEM-QEMU-030116/107

			infinite loop issue. It could occur while receiving packets in 'mcf_fec_receive'. A privileged user/process inside guest could use this issue to crash the QEMU process on the host leading to DoS. **REFERENCE: CVE-2016-9776**	29	
NA	29-12-2016	2.1	QEMU (aka Quick Emulator) built with the USB EHCI emulation support is vulnerable to a null pointer dereference flaw. It could occur when an application attempts to write to EHCI capabilities registers. A privileged user inside quest could use this flaw to crash the QEMU process instance resulting in DoS. **REFERENCE: CVE-2016-2198**	https://bugzilla.redhat.com/show_bug.cgi?id=1301643	A-QEM-QEMU-030116/108
NA	29-12-2016	2.1	QEMU (aka Quick Emulator) built with an IDE AHCI emulation support is vulnerable to a null pointer dereference flaw. It occurs while unmapping the Frame Information Structure (FIS) and Command List Block (CLB) entries. A privileged user inside guest could use this flaw to crash the QEMU process instance resulting in DoS. **REFERENCE: CVE-2016-2197**	https://bugzilla.redhat.com/show_bug.cgi?id=1302057	A-QEM-QEMU-030116/109
NA	29-12-2016	2.1	QEMU (aka Quick Emulator) built with the e1000 NIC emulation support is vulnerable to an infinite loop issue. It could occur while processing data via transmit or receive descriptors, provided the initial receive/transmit descriptor head (TDH/RDH) is set outside the allocated descriptor buffer. A privileged	https://bugzilla.redhat.com/show_bug.cgi?id=1298570	A-QEM-QEMU-030116/110

			user inside guest could use this flaw to crash the QEMU instance resulting in DoS. **REFERENCE: CVE-2016-1981**		
NA	29-12-2016	2.1	QEMU (aka Quick Emulator) built with the TPR optimization for 32-bit Windows guests support is vulnerable to a null pointer dereference flaw. It occurs while doing I/O port write operations via hmp interface. In that, 'current_cpu' remains null, which leads to the null pointer dereference. A user or process could use this flaw to crash the QEMU instance, resulting in DoS issue. **REFERENCE: CVE-2016-1922**	https://bugzilla.redhat.com/show_bug.cgi?id=1283934	A-QEM-QEMU-030116/111
Denial of Service	29-12-2016	2.1	The cpu_physical_memory_write_rom_internal function in exec.c in QEMU (aka Quick Emulator) does not properly skip MMIO regions, which allows local privileged guest users to cause a denial of service (guest crash) via unspecified vectors. **CVE-2015-8818**	https://bugzilla.redhat.com/show_bug.cgi?id=1300771	A-QEM-QEMU-030116/112
NA	29-12-2016	2.1	QEMU (aka Quick Emulator) built with a VMWARE VMXNET3 paravirtual NIC emulator support is vulnerable to crash issue. It could occur while reading Interrupt Mask Registers (IMR). A privileged (CAP_SYS_RAWIO) guest user could use this flaw to crash the QEMU process instance resulting in DoS. **CVE-2015-8745**	https://bugzilla.redhat.com/show_bug.cgi?id=1270876	A-QEM-QEMU-030116/113
NA	29-12-2016	2.1	QEMU (aka Quick Emulator) built with a VMWARE VMXNET3 paravirtual NIC emulator support is vulnerable	http://git.qemu.org/?p=qemu.git;a=commitdiff;h=a	A-QEM-QEMU-030116/114

			to crash issue. It occurs when a guest sends a Layer-2 packet smaller than 22 bytes. A privileged (CAP_SYS_RAWIO) guest user could use this flaw to crash the QEMU process instance resulting in DoS. **CVE-2015-8744**	7278b36fcab9af469563bd7b	
NA	29-12-2016	3.6	QEMU (aka Quick Emulator) built with the NE2000 device emulation support is vulnerable to an OOB r/w access issue. It could occur while performing 'ioport' r/w operations. A privileged (CAP_SYS_RAWIO) user/process could use this flaw to leak or corrupt QEMU memory bytes. **CVE-2015-8743**	https://bugzilla.redhat.com/show_bug.cgi?id=1264929	A-QEM-QEMU-030116/115
NA	29-12-2016	2.1	QEMU (aka Quick Emulator) built with the Rocker switch emulation support is vulnerable to an off-by-one error. It happens while processing transmit (tx) descriptors in 'tx_consume' routine, if a descriptor was to have more than allowed (ROCKER_TX_FRAGS_MAX=16) fragments. A privileged user inside guest could use this flaw to cause memory leakage on the host or crash the QEMU process instance resulting in DoS issue. **CVE-2015-8701**	https://bugzilla.redhat.com/show_bug.cgi?id=1286971	A-QEM-QEMU-030116/116
Rapid7					
Nexpose Rapid7 Nexpose is a vulnerability scanner which aims to support the entire vulnerability management lifecycle, including discovery, detection, verification, risk classification, impact analysis, reporting and mitigation.					
Cross Site Scripting	20-12-2016	3.5	In the Create Tags page of the Rapid7 Nexpose version 6.4.12 user interface, any	https://help.rapid7.com/nexpose/en-	A-RAP-NEXPO-030116/117

			authenticated user who has the capability to create tags can inject cross-site scripting (XSS) elements in the tag name field. Once this tag is viewed in the Tag Detail page of the Rapid7 Nexpose 6.4.12 UI by another authenticated user, the script is run in that user's browser context. **REFERENCE: CVE-2016-9757**	us/release-notes/#6.4.13	
Roundcube					
Webmail Roundcube webmail is a free and open source webmail software for the masses, written in PHP.					
Cross Site Scripting	20-12-2016	4.3	Cross-site scripting (XSS) vulnerability in Roundcube Webmail before 1.2.0 allows remote attackers to inject arbitrary web script or HTML via the href attribute in an area tag in an e-mail message. **REFERENCE: CVE-2016-4552**	https://github.com/roundcube/roundcubemail/issues/5240	A-ROU-WEBMA-030116/118
Cross Site Scripting	20-12-2016	4.3	Cross-site scripting (XSS) vulnerability in Roundcube Webmail before 1.2.0 allows remote attackers to inject arbitrary web script or HTML via the href attribute in an area tag in an e-mail message. **REFERENCE: CVE-2016-4552**	NA	A-ROU-WEBMA-030116/119
S9Y					
Serendipity Serendipity is a PHP-powered weblog engine which gives the user an easy way to maintain a blog.					
Cross Site Scripting	25-12-2016	3.5	Multiple cross-site scripting (XSS) vulnerabilities in Serendipity before 2.0.5 allow remote authenticated users to inject arbitrary web script or HTML via a category or directory name. **REFERENCE: CVE-2016-9681**	NA	A-S9Y-SEREN-030116/120
Siemens					
Desigo Web Module Pxa30-w0 Firmware;Desigo Web Module Pxa30-w1 Firmware;Desigo Web Module Pxa30-w2 Firmware;Desigo Web Module Pxa40-w0 Firmware;Desigo Web Module Pxa40-					

w1 Firmware;Desigo Web Module Pxa40-w2 Firmware NA					
NA	23-12-2016	5	Siemens Desigo PX Web modules PXA40-W0, PXA40-W1, PXA40-W2 for Desigo PX automation controllers PXC00-E.D, PXC50-E.D, PXC100-E.D, PXC200-E.D (All firmware versions < V6.00.046) and Desigo PX Web modules PXA30-W0, PXA30-W1, PXA30-W2 for Desigo PX automation controllers PXC00-U, PXC64-U, PXC128-U (All firmware versions < V6.00.046) use a pseudo random number generator with insufficient entropy to generate certificates for HTTPS, potentially allowing remote attackers to reconstruct the corresponding private key. **REFERENCE: CVE-2016-9154**	NA	A-SIE-DESIG-030116/121
Simatic Pcs 7;Simatic Wincc SIMATIC PCS 7 has everything you need to completely and safely automate your entire production process, from goods receipt to goods issue, in both manufacturing and process plants; SIMATIC WinCC is a supervisory control and data acquisition (SCADA) and human-machine interface (HMI) system from Siemens.					
NA	16-12-2016	5.8	A vulnerability in SIEMENS SIMATIC WinCC (All versions < SIMATIC WinCC V7.2) and SIEMENS SIMATIC PCS 7 (All versions < SIMATIC PCS 7 V8.0 SP1) could allow a remote attacker to crash an ActiveX component or leak parts of the application memory if a user is tricked into clicking on a malicious link under certain conditions. **REFERENCE: CVE-2016-9160**	http://www.siemens.com/cert/pool/cert/siemens_security_advisory_ssa-693129.pdf	A-SIE-SIMAT-030116/122

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Tarantool					
Msgpuck msgpuck is a simple and efficient MsgPack binary serialization library in a self-contained header file.					
Denial of Service	23-12-2016	5	An exploitable incorrect return value vulnerability exists in the mp_check function of Tarantool's Msgpuck library 1.0.3. A specially crafted packet can cause the mp_check function to incorrectly return success when trying to check if decoding a map16 packet will read outside the bounds of a buffer, resulting in a denial of service vulnerability. **REFERENCE: CVE-2016-9036**	NA	A-TAR-MSGPU-030116/123
Tarantool Tarantool is an open-source NoSQL database management system and Lua application server.					
Denial of Service	23-12-2016	7.8	An exploitable out-of-bounds array access vulnerability exists in the xrow_header_decode function of Tarantool 1.7.2.0-g8e92715. A specially crafted packet can cause the function to access an element outside the bounds of a global array that is used to determine the type of the specified key's value. This can lead to an out of bounds read within the context of the server. An attacker who exploits this vulnerability can cause a denial of service vulnerability on the server. **REFERENCE: CVE-2016-9037**	NA	A-TAR-TARAN-030116/124
Vmware					
Fusion VMware Fusion is the easiest, fastest and most reliable way to run Windows applications on a Mac without rebooting.					
Bypass; Gain Information	29-12-2016	2.1	VMware Fusion 8.x before 8.5 on OS X, when System Integrity Protection (SIP) is enabled, allows local users to determine	http://www.vmware.com/security/advisories/VMS	A-VMW-FUSIO-030116/125

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			kernel memory addresses and bypass the kASLR protection mechanism via unspecified vectors. **REFERENCE: CVE-2016-5329**	A-2016-0017.html	
Fusion; Fusion Pro; Workstation Player; Workstation Pro VMware Fusion Pro and VMware Fusion let anyone run Windows and hundreds of other operating systems on a Mac, without rebooting; VMware Workstation Pro and VMware Workstation Player are the industry standard for running multiple operating systems as virtual machines on a single PC.					
Denial of Service, Execute Code; Overflow	29-12-2016	7.2	The drag-and-drop (aka DnD) function in VMware Workstation Pro 12.x before 12.5.2 and VMware Workstation Player 12.x before 12.5.2 and VMware Fusion and Fusion Pro 8.x before 8.5.2 allows guest OS users to execute arbitrary code on the host OS or cause a denial of service (out-of-bounds memory access on the host OS) via unspecified vectors. **REFERENCE: CVE-2016-7461**	http://www.vmware.com/security/advisories/VMSA-2016-0019.html	A-VMW-FUSIO-030116/126
Horizon View VMware Horizon View is the virtual desktop host platform for vSphere.					
Directory Traversal; Gain Information	29-12-2016	5	Directory traversal vulnerability in the Connection Server in VMware Horizon View 5.x before 5.3.7, 6.x before 6.2.3, and 7.x before 7.0.1 allows remote attackers to obtain sensitive information via unspecified vectors. **REFERENCE: CVE-2016-7087**	http://www.vmware.com/security/advisories/VMSA-2016-0015.html	A-VMW-HORIZ-030116/127
Identity Manger; Vrealize Automation VMware Identity Manager Enables Identity Management for the Mobile Cloud Era; vRealize Automation cloud automation software automates the delivery of IT services.					
NA	29-12-2016	5	VMware Identity Manager 2.x before 2.7.1 and vRealize Automation 7.x before 7.2.0 allow remote attackers to read /SAAS/WEB-INF and /SAAS/META-INF files via unspecified vectors. **REFERENCE: CVE-2016-5334**	http://www.vmware.com/security/advisories/VMSA-2016-0021.html	A-VMW-IDENT-030116/128

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Tools VMware Tools is an optional, free set of drivers and utilities that enhances both the performance of a virtual machine's guest operating system and interaction between the guest and the host.					
Denial of Service; Gain Privileges	29-12-2016	4.6	The graphic acceleration functions in VMware Tools 9.x and 10.x before 10.0.9 on OS X allow local users to gain privileges or cause a denial of service (NULL pointer dereference) via unspecified vectors, a different vulnerability than CVE-2016-7079. **REFERENCE: CVE-2016-7080**	http://www.vmware.com/security/advisories/VMSA-2016-0014.html	A-VMW-TOOLS-030116/129
Denial of Service; Gain Privileges	29-12-2016	4.6	The graphic acceleration functions in VMware Tools 9.x and 10.x before 10.0.9 on OS X allow local users to gain privileges or cause a denial of service (NULL pointer dereference) via unspecified vectors, a different vulnerability than CVE-2016-7080. **REFERENCE: CVE-2016-7079**	http://www.vmware.com/security/advisories/VMSA-2016-0014.html	A-VMW-TOOLS-030116/130
Bypass	29-12-2016	2.1	VMware Tools 9.x and 10.x before 10.1.0 on OS X, when System Integrity Protection (SIP) is enabled, allows local users to determine kernel memory addresses and bypass the kASLR protection mechanism via unspecified vectors. **REFERENCE: CVE-2016-5328**	http://www.vmware.com/security/advisories/VMSA-2016-0017.html	A-VMW-TOOLS-030116/131
Vcenter Server VMware vCenter server is a centralized management application that lets you manage virtual machines and ESXi hosts centrally.					
NA	29-12-2016	4	VMware vCenter Server 5.5 before U3e and 6.0 before U2a allows remote authenticated users to read arbitrary files via a (1) Log Browser, (2) Distributed Switch setup, or (3) Content Library XML	http://www.vmware.com/security/advisories/VMSA-2016-0022.html	A-VMW-VCENT-030116/132

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			document containing an external entity declaration in conjunction with an entity reference, related to an XML External Entity (XXE) issue. **REFERENCE: CVE-2016-7459**		
Vrealize Automation VMware vRealize Automation, formerly called vCloud Automation Center, is a software product for unified cloud management.					
Denial of Service	29-12-2016	6.4	The Single Sign-On feature in VMware vCenter Server 5.5 before U3e and 6.0 before U2a and vRealize Automation 6.x before 6.2.5 allows remote attackers to read arbitrary files or cause a denial of service via an XML document containing an external entity declaration in conjunction with an entity reference, related to an XML External Entity (XXE) issue. **REFERENCE: CVE-2016-7460**	http://www.vmware.com/security/advisories/VMSA-2016-0022.html	A-VMW-VREAL-030116/133
Vrealize Operations vRealize Operations is available in three editions (Standard, Advanced and Enterprise) for teams responsible for managing vSphere and virtual infrastructure, heterogeneous virtual and physical environments, or multi-cloud infrastructure at the OS and application level.					
NA	29-12-2016	7.5	The Suite REST API in VMware vRealize Operations (aka vROps) 6.x before 6.4.0 allows remote authenticated users to write arbitrary content to files or rename files via a crafted DiskFileItem in a relay-request payload that is mishandled during deserialization. **REFERENCE: CVE-2016-7462**	http://www.vmware.com/security/advisories/VMSA-2016-0020.html	A-VMW-VREAL-030116/134
Gain Privileges	29-12-2016	8	VMware vRealize Operations (aka vROps) 6.x before 6.4.0 allows remote authenticated users to gain privileges, or halt and remove virtual machines, via unspecified vectors. **REFERENCE: CVE-2016-7457**	http://www.vmware.com/security/advisories/VMSA-2016-0016.html	A-VMW-VREAL-030116/135
Vsphere Client VMware vSphere client is a Windows application for administering VMware vCenter Server and					

VMware ESX/ESXi virtualization platforms.					
NA	29-12-2016	5	VMware vSphere Client 5.5 before U3e and 6.0 before U2a allows remote vCenter Server and ESXi instances to read arbitrary files via an XML document containing an external entity declaration in conjunction with an entity reference, related to an XML External Entity (XXE) issue. **REFERENCE: CVE-2016-7458**	http://www.vmware.com/security/advisories/VMSA-2016-0022.html	A-VMW-VSPHE-030116/136
Vsphere Data Protection VDP is a robust, simple-to-deploy, disk-based backup and recovery solution.					
NA	29-12-2016	10	VMware vSphere Data Protection (VDP) 5.5.x though 6.1.x has an SSH private key with a publicly known password, which makes it easier for remote attackers to obtain login access via an SSH session. **REFERENCE: CVE-2016-7456**	http://www.vmware.com/security/advisories/VMSA-2016-0024.html	A-VMW-VSPHE-030116/137
Workstation Player; Workstation Pro VMware Workstation Pro and VMware Workstation Player are the industry standard for running multiple operating systems as virtual machines on a single PC.					
Gain Privileges	29-12-2016	7.2	The installer in VMware Workstation Pro 12.x before 12.5.0 and VMware Workstation Player 12.x before 12.5.0 on Windows allows local users to gain privileges via a Trojan horse setup64.exe file in the installation directory. **REFERENCE: CVE-2016-7086**	http://www.vmware.com/security/advisories/VMSA-2016-0014.html	A-VMW-WORKS-030116/138
Gain Privileges	29-12-2016	7.2	Untrusted search path vulnerability in the installer in VMware Workstation Pro 12.x before 12.5.0 and VMware Workstation Player 12.x before 12.5.0 on Windows allows local users to gain privileges via a Trojan horse DLL in an unspecified directory.	http://www.vmware.com/security/advisories/VMSA-2016-0014.html	A-VMW-WORKS-030116/139

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			REFERENCE: CVE-2016-7085		
Denial of Service; Execute Code; Overflow; Memory Corruption	29-12-2016	6.9	tpview.dll in VMware Workstation Pro 12.x before 12.5.0 and VMware Workstation Player 12.x before 12.5.0 on Windows, when Cortado ThinPrint virtual printing is enabled, allows guest OS users to execute arbitrary code on the host OS or cause a denial of service (host OS memory corruption) via a JPEG 2000 image. **REFERENCE: CVE-2016-7084**	http://www.vmware.com/security/advisories/VMSA-2016-0014.html	A-VMW-WORKS-030116/140
Denial of Service; Execute Code; Overflow; Memory Corruption	29-12-2016	5.9	VMware Workstation Pro 12.x before 12.5.0 and VMware Workstation Player 12.x before 12.5.0 on Windows, when Cortado ThinPrint virtual printing is enabled, allow guest OS users to execute arbitrary code on the host OS or cause a denial of service (host OS memory corruption) via TrueType fonts embedded in EMFSPOOL. **REFERENCE: CVE-2016-7083**	http://www.vmware.com/security/advisories/VMSA-2016-0014.html	A-VMW-WORKS-030116/141
Denial of Service; Execute Code; Overflow; Memory Corruption	29-12-2016	5.9	VMware Workstation Pro 12.x before 12.5.0 and VMware Workstation Player 12.x before 12.5.0 on Windows, when Cortado ThinPrint virtual printing is enabled, allow guest OS users to execute arbitrary code on the host OS or cause a denial of service (host OS memory corruption) via an EMF file. **REFERENCE: CVE-2016-7082**	http://www.vmware.com/security/advisories/VMSA-2016-0014.html	A-VMW-WORKS-030116/142
Execute Code; Overflow	29-12-2016	6.9	Multiple heap-based buffer overflows in VMware Workstation Pro 12.x before 12.5.0 and VMware Workstation Player 12.x before 12.5.0 on Windows, when	http://www.vmware.com/security/advisories/VMSA-2016-0014.html	A-VMW-WORKS-030116/143

			Cortado ThinPrint virtual printing is enabled, allow guest OS users to execute arbitrary code on the host OS via unspecified vectors. **REFERENCE: CVE-2016-7081**		
Xmltwig					
Xml-twig For Perl XML::Twig is a Perl module used to process efficiently XML documents					
NA	22-12-2016	6.4	perl-XML-Twig: The option to `expand_external_ents`, documented as controlling external entity expansion in XML::Twig does not work. External entities are always expanded, regardless of the option's setting. **REFERENCE: CVE-2016-9180**	NA	A-XML-XML-T-030116/144
Application; Operating System (A/OS)					
Debian/Xrdp					
Debian Linux/Xrdp Debian is an operating system and a distribution of Free Software/ xrdp is an open source RDP server.					
NA	16-12-2016	5	An issue was discovered in xrdp before 0.9.1. When successfully logging in using RDP into an xrdp session, the file ~/.vnc/sesman_${username}_passwd is created. Its content is the equivalent of the user's cleartext password, DES encrypted with a known key. **REFERENCE: CVE-2013-1430**	https://github.com/neutrinolabs/xrdp/pull/497	A-OS-DEB-DEBIA-030116/145
Debian; Fedoraproject; Suse/KDE					
Debian Linux/Fedora/Linux Enterprise/Kmail Debian is an operating system and a distribution of Free Software/ Fedora (formerly Fedora Core) is an operating system based on the Linux kernel, developed by the community-supported Fedora Project and sponsored by Red Hat/SUSE Linux Enterprise Server is a world-class, secure open source server operating system, built to power physical, virtual and cloud-based mission-critical workloads/ KMail is the email component of Kontact, the integrated personal information manager from KDE.					
NA	23-12-2016	7.5	Through a malicious URL that contained a quote character it was possible to inject HTML code in KMail's plaintext	NA	A-OS-DEB-DEBIA-030116/146

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			viewer. Due to the parser used on the URL it was not possible to include the equal sign (=) or a space into the injected HTML, which greatly reduces the available HTML functionality. Although it is possible to include an HTML comment indicator to hide content. **REFERENCE: CVE-2016-7966**		
Fedoraproject; Novell/KDE					
Fedora/Leap/Kscreenlocker; Plasma-workspace Fedora (formerly Fedora Core) is an operating system based on the Linux kernel, developed by the community-supported Fedora Project and sponsored by Red Hat/ LEAP is an online community for energy analysts working for sustainability and the home of the LEAP software system/ Kscreenlocker can be configured to support the PAM (Pluggable Authentication Modules) system for password checking (for unlocking the display).					
Denial of Service	23-12-2016	4.6	Turning all screens off in Plasma-workspace and kscreenlocker while the lock screen is shown can result in the screen being unlocked when turning a screen on again. **REFERENCE: CVE-2016-2312**	NA	A-OS-FED-FEDOR-030116/147
NA	23-12-2016	4.6	Turning all screens off in Plasma-workspace and kscreenlocker while the lock screen is shown can result in the screen being unlocked when turning a screen on again. **REFERENCE: CVE-2016-2312**	https://www.kde.org/info/security/advisory-20160209-1.txt	A-OS-FED-FEDOR-030116/148
KDE/Novell;Opensuse Project					
Kde-cli-tools/Leap/Opensuse Kde-cli-tools are tools based on KDE Frameworks 5 to better interact with the system/ LEAP is an online community for energy analysts working for sustainability and the home of the LEAP software system/ openSUSE, formerly SUSE Linux and SuSE Linux Professional, is a Linux-based project and distribution sponsored by SUSE Linux GmbH and other companies.					
Execute Code	23-12-2016	4	A maliciously crafted command line for kdesu can result in the user only seeing part of the commands that will actually get executed as super user.	NA	A-OS-KDE-KDE-C-030116/149

			REFERENCE: CVE-2016-7787		
Microsoft/Microsoft					
Office For Mac/Windows 7;Windows Server 2008;Windows Vista Microsoft Office 2016 for Mac is by far the most powerful set of productivity apps for Apple computers/Windows 7 (codenamed Vienna, formerly Blackcomb) is a personal computer operating system developed by Microsoft; Windows Server 2008 is one of Microsoft Windows' server line of operating systems; Windows Vista is the 6th version of the Microsoft Windows operating system from Microsoft.					
Gain Information	20-12-2016	4.3	The GDI component in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Office for Mac 2011, and Office 2016 for Mac allows remote attackers to obtain sensitive information from process memory via a crafted web site, aka "GDI Information Disclosure Vulnerability." **REFERENCE: CVE-2016-7257**	NA	A-OS-MIC-OFFIC-030116/150
Operating System (OS)					
Blackberry					
Good Enterprise Mobility Server Good Enterprise Mobility Server (GEMS) consolidates the Good Connect and Good Mobile Messaging servers into modules on a standardized architecture.					
Execute Code	16-12-2016	8.5	Remote shell execution vulnerability in the BlackBerry Good Enterprise Mobility Server (GEMS) implementation of the Apache Karaf command shell in GEMS versions 2.1.5.3 to 2.2.22.25 allows remote attackers to obtain local administrator rights on the GEMS server via commands executed on the Karaf command shell. **REFERENCE: CVE-2016-3129**	http://support.blackberry.com/kb/articleDetail?articleNumber=000038814&language=None	O-BLA-GOOD - 030116/151
Execute Code	16-12-2016	8.5	Remote shell execution vulnerability in the BlackBerry Good Enterprise Mobility Server (GEMS) implementation of the Apache Karaf command shell in GEMS versions 2.1.5.3	http://support.blackberry.com/kb/articleDetail?articleNumber=000038814&l	O-BLA-GOOD - 030116/152

			to 2.2.22.25 allows remote attackers to obtain local administrator rights on the GEMS server via commands executed on the Karaf command shell. **REFERENCE: CVE-2016-3129**	anguage=None	
Google					
Android Android is a mobile operating system developed by Google, based on the Linux kernel and designed primarily for touchscreen mobile devices such as smartphones and tablets.					
Gain Information	23-12-2016	4.3	The non-existent notification listener vulnerability was introduced in the initial Android 5.0.2 builds for the Samsung Galaxy S6 Edge devices, but the vulnerability can persist on the device even after the device has been upgraded to an Android 5.1.1 or 6.0.1 build. The vulnerable system app gives a non-existent app the ability to read the notifications from the device, which a third-party app can utilize if it uses a package name of com.samsung.android.app.portalservicewidget. This vulnerability allows an unprivileged third-party app to obtain the text of the user's notifications, which tend to contain personal data. **REFERENCE: CVE-2016-6910**	NA	O-GOO-ANDRO-030116/153
HP					
Thinpro HP ThinPro OS is the out-of-the-box OS for HP Thin Clients.					
Gain Privileges; Bypass	29-12-2016	7.2	HP ThinPro 4.4 through 6.1 mishandles the keyboard layout control panel and virtual keyboard application, which allows local users to bypass intended access restrictions and gain privileges	NA	O-HP-THINP-030116/154

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			via unspecified vectors. **REFERENCE: CVE-2016-2246**		
Gain Privileges; Bypass	29-12-2016	7.2	HP ThinPro 4.4 through 6.1 mishandles the keyboard layout control panel and virtual keyboard application, which allows local users to bypass intended access restrictions and gain privileges via unspecified vectors. **REFERENCE: CVE-2016-2246**	NA	O-HP-THINP-030116/155
Linux					
Linux Kernel Linux Kernel in a Nutshell is a comprehensive overview of kernel configuration and building, a critical task for Linux users and administrators.					
Denial of Service	28-12-2016	7.2	Race condition in the netlink_dump function in net/netlink/af_netlink.c in the Linux kernel before 4.6.3 allows local users to cause a denial of service (double free) or possibly have unspecified other impact via a crafted application that makes sendmsg system calls, leading to a free operation associated with a new dump that started earlier than anticipated. **REFERENCE: CVE-2016-9806**	https://bugzilla.redhat.com/show_bug.cgi?id=1401502	O-LIN-LINUX-030116/156
Denial of Service	28-12-2016	4.6	Race condition in the snd_pcm_period_elapsed function in sound/core/pcm_lib.c in the ALSA subsystem in the Linux kernel before 4.7 allows local users to cause a denial of service (use-after-free) or possibly have unspecified other impact via a crafted SNDRV_PCM_TRIGGER_START command. **REFERENCE: CVE-2016-9794**	https://bugzilla.redhat.com/show_bug.cgi?id=1401494	O-LIN-LINUX-030116/157
Denial of Service; Overflow;	28-12-2016	7.2	The sock_setsockopt function in net/core/sock.c in the Linux kernel before 4.8.14	http://git.kernel.org/cgit/linux/kernel/	O-LIN-LINUX-030116/158

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Memory Corruption			mishandles negative values of sk_sndbuf and sk_rcvbuf, which allows local users to cause a denial of service (memory corruption and system crash) or possibly have unspecified other impact by leveraging the CAP_NET_ADMIN capability for a crafted setsockopt system call with the (1) SO_SNDBUFFORCE or (2) SO_RCVBUFFORCE option. **REFERENCE: CVE-2016-9793**	git/torvalds/linux.git/commit/?id=b98b0bc8c431e3ceb4b26b0dfc8db509518fb290	
Denial of Service, Gain Privileges	28-12-2016	6.9	KVM in the Linux kernel before 4.8.12, when I/O APIC is enabled, does not properly restrict the VCPU index, which allows guest OS users to gain host OS privileges or cause a denial of service (out-of-bounds array access and host OS crash) via a crafted interrupt request, related to arch/x86/kvm/ioapic.c and arch/x86/kvm/ioapic.h. **REFERENCE: CVE-2016-9777**	http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=81cdb259fb6d8c1c4ecfeea389ff5a73c07f5755	O-LIN-LINUX-030116/159
Gain Information	28-12-2016	2.1	arch/x86/kvm/emulate.c in the Linux kernel before 4.8.12 does not properly initialize Code Segment (CS) in certain error cases, which allows local users to obtain sensitive information from kernel stack memory via a crafted application. **REFERENCE: CVE-2016-9756**	https://github.com/torvalds/linux/commit/2117d5398c81554fbf803f5fd1dc55eb78216c0c	O-LIN-LINUX-030116/160
Denial of Service; Overflow	28-12-2016	4.6	The netfilter subsystem in the Linux kernel before 4.9 mishandles IPv6 reassembly, which allows local users to cause a denial of service (integer overflow, out-of-bounds write, and GPF) or possibly have unspecified	https://github.com/torvalds/linux/commit/9b57da0630c9fd36ed7a20fc0f98dc82cc0777fa	O-LIN-LINUX-030116/161

			other impact via a crafted application that makes socket, connect, and writev system calls, related to net/ipv6/netfilter/nf_conntrack_reasm.c and net/ipv6/netfilter/nf_defrag_ipv6_hooks.c. **REFERENCE: CVE-2016-9755**		
Denial of Service	28-12-2016	4.9	Multiple memory leaks in error paths in fs/xfs/xfs_attr_list.c in the Linux kernel before 4.5.1 allow local users to cause a denial of service (memory consumption) via crafted XFS filesystem operations. **REFERENCE: CVE-2016-9685**	http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=2e83b79b2d6c78bf1b4aa227938a214dcbddc83f	O-LIN-LINUX-030116/162
Denial of Service	28-12-2016	2.1	arch/x86/kvm/vmx.c in the Linux kernel through 4.9 mismanages the #BP and #OF exceptions, which allows guest OS users to cause a denial of service (guest OS crash) by declining to handle an exception thrown by an L2 guest. **REFERENCE: CVE-2016-9588**	http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=ef85b67385436ddc1998f45f1d6a210f935b3388	O-LIN-LINUX-030116/163
Denial of Service	28-12-2016	7.2	The blk_rq_map_user_iov function in block/blk-map.c in the Linux kernel before 4.8.14 does not properly restrict the type of iterator, which allows local users to read or write to arbitrary kernel memory locations or cause a denial of service (use-after-free) by leveraging access to a /dev/sg device. **REFERENCE: CVE-2016-9576**	http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=a0ac402cfcdc904f9772e1762b3fda112dcc56a0	O-LIN-LINUX-030116/164
Gain Privileges	28-12-2016	6.9	kernel/events/core.c in the performance subsystem in the Linux kernel before 4.0 mismanages locks during	http://git.kernel.org/cgit/linux/kernel/git/torvalds/	O-LIN-LINUX-030116/165

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			certain migrations, which allows local users to gain privileges via a crafted application, aka Android internal bug 31095224. **REFERENCE: CVE-2016-6787**	linux.git/commit/?id=f63a8daa5812afef4f06c962351687e1ff9ccb2b	
Gain Privileges	28-12-2016	6.9	kernel/events/core.c in the performance subsystem in the Linux kernel before 4.0 mismanages locks during certain migrations, which allows local users to gain privileges via a crafted application, aka Android internal bug 30955111. **REFERENCE: CVE-2016-6786**	http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=f63a8daa5812afef4f06c962351687e1ff9ccb2b	O-LIN-LINUX-030116/166
Denial of Service	28-12-2016	4.7	fs/namespace.c in the Linux kernel before 4.9 does not restrict how many mounts may exist in a mount namespace, which allows local users to cause a denial of service (memory consumption and deadlock) via MS_BIND mount system calls, as demonstrated by a loop that triggers exponential growth in the number of mounts. **REFERENCE: CVE-2016-6213**	https://github.com/torvalds/linux/commit/d29216842a85c7970c536108e093963f02714498	O-LIN-LINUX-030116/167
Denial of Service; Overflow; Memory Corruption	28-12-2016	7.2	The sock_setsockopt function in net/core/sock.c in the Linux kernel before 3.5 mishandles negative values of sk_sndbuf and sk_rcvbuf, which allows local users to cause a denial of service (memory corruption and system crash) or possibly have unspecified other impact by leveraging the CAP_NET_ADMIN capability for a crafted setsockopt system call with the (1) SO_SNDBUF or (2) SO_RCVBUF option. **CVE-2012-6704**	http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=82981930125abfd39d7c8378a9cfdf5e1be2002b	O-LIN-LINUX-030116/168

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Microsoft					
Windows 10;Windows 7;Windows 8.1;Windows Rt 8.1;Windows Server 2008;Windows Server 2012;Windows Server 2016;Windows Vista Microsoft Windows is a meta-family of graphical operating systems developed, marketed, and sold by Microsoft. It consists of several families of operating systems which cater to a certain sector of the computing industry with the OS typically associated with IBM PC compatible architecture.					
Gain Information	20-12-2016	2.1	The Common Log File System (CLFS) driver in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 allows local users to obtain sensitive information from process memory via a crafted application, aka "Windows Common Log File System Driver Information Disclosure Vulnerability." **REFERENCE: CVE-2016-7295**	NA	O-MIC-WINDO-030116/169
Gain Privileges	20-12-2016	7.2	The Installer in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 mishandles library loading, which allows local users to gain privileges via a crafted application, aka "Windows Installer Elevation of Privilege Vulnerability." **REFERENCE: CVE-2016-7292**	NA	O-MIC-WINDO-030116/170
Execute Code	20-12-2016	9.3	Uniscribe in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and	NA	O-MIC-WINDO-030116/171

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			1607, and Windows Server 2016 allows remote attackers to execute arbitrary code via a crafted web site, aka "Windows Uniscribe Remote Code Execution Vulnerability." **REFERENCE: CVE-2016-7274**		
Execute Code	20-12-2016	9.3	The Graphics component in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 allows remote attackers to execute arbitrary code via a crafted web site, aka "Windows Graphics Remote Code Execution Vulnerability." **REFERENCE: CVE-2016-7272**	NA	O-MIC-WINDO-030116/172
Gain Privileges	20-12-2016	7.2	The kernel-mode drivers in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 allow local users to gain privileges via a crafted application, aka "Win32k Elevation of Privilege Vulnerability." **REFERENCE: CVE-2016-7260**	NA	O-MIC-WINDO-030116/173
Gain Privileges	20-12-2016	7.2	The Graphics Component in the kernel-mode drivers in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 allows local users	NA	O-MIC-WINDO-030116/174

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			to gain privileges via a crafted application, aka "Win32k Elevation of Privilege Vulnerability." **REFERENCE: CVE-2016-7259**		
Gain Information	20-12-2016	2.1	The Crypto driver in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 allows local users to obtain sensitive information via a crafted application, aka "Windows Crypto Driver Information Disclosure Vulnerability." **REFERENCE: CVE-2016-7219**	NA	O-MIC-WINDO-030116/175
Execute Code	20-12-2016	9.3	The Graphics component in Microsoft Windows 10 Gold, 1511, and 1607 and Windows Server 2016 allows remote attackers to execute arbitrary code via a crafted web site, aka "Windows Graphics Remote Code Execution Vulnerability." **REFERENCE: CVE-2016-7273**	NA	O-MIC-WINDO-030116/176
Bypass	20-12-2016	4.6	The Secure Kernel Mode implementation in Microsoft Windows 10 Gold, 1511, and 1607 and Windows Server 2016 allows local users to bypass the virtual trust level (VTL) protection mechanism via a crafted application, aka "Secure Kernel Mode Elevation of Privilege Vulnerability." **REFERENCE: CVE-2016-7271**	NA	O-MIC-WINDO-030116/177
Gain Information	20-12-2016	2.1	The kernel in Microsoft Windows 10 Gold, 1511, and 1607 and Windows Server 2016 mishandles page-fault system calls, which allows	NA	O-MIC-WINDO-030116/178

			local users to obtain sensitive information from arbitrary processes via a crafted application, aka "Windows Kernel Memory Address Information Disclosure Vulnerability." **REFERENCE: CVE-2016-7258**		
Redhat					
Enterprise Linux;Enterprise Linux Desktop;Enterprise Linux Hpc Node;Enterprise Linux Server;Enterprise Linux Workstation Red Hat Enterprise Linux (RHEL) is a Linux distribution developed by Red Hat and targeted toward the commercial market.					
Gain Information	22-12-2016	4.9	sudo: It was discovered that the default sudo configuration on Red Hat Enterprise Linux and possibly other Linux implementations preserves the value of INPUTRC which could lead to information disclosure. A local user with sudo access to a restricted program that uses readline could use this flaw to read content from specially formatted files with elevated privileges provided by sudo. **REFERENCE: CVE-2016-7091**	NA	O-RED-ENTER-030116/179
Siemens					
Simatic S7-300 Cpu Firmware;Simatic S7-400 Cpu Firmware NA					
Gain Information	16-12-2016	4.3	A vulnerability in SIEMENS SIMATIC S7-300 PN CPUs (all versions including V3.2.12) and SIMATIC S7-400 PN CPUs (all versions including V7) could allow a remote attacker to obtain credentials from the PLC if protection-level 2 is configured on the affected devices. **REFERENCE: CVE-2016-9159**	http://www.siemens.com/cert/pool/cert/siemens_security_advisory_ssa-731239.pdf	O-SIE-SIMAT-030116/180
Denial of Service	16-12-2016	7.8	A vulnerability in SIEMENS SIMATIC S7-300 PN CPUs (all versions including V3.2.12)	http://www.siemens.com/cert/pool/c	O-SIE-SIMAT-030116/181

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			and SIMATIC S7-400 PN CPUs (V6 and V7) could allow a remote attacker to cause a Denial of Service condition by sending specially crafted packets to port 80/TCP. **REFERENCE: CVE-2016-9158**	ert/siemens_security_advisory_ssa-731239.pdf	
Technicolor					
Xfinity Gateway Router Dpc3941t Firmware NA					
Cross Site Request Forgery	16-12-2016	7.9	CSRF vulnerability on Technicolor TC dpc3941T (formerly Cisco dpc3941T) devices with firmware dpc3941-P20-18-v303r20421733-160413a-CMCST allows an attacker to change the Wi-Fi password, open the remote management interface, or reset the router. **REFERENCE: CVE-2016-7454**	NA	O-TEC-XFINI-030116/182
Vmware					
Esxi VMware ESXi is the industry-leading, purpose-built bare-metal hypervisor.					
Cross Site Scripting	29-12-2016	3.5	Cross-site scripting (XSS) vulnerability in the Host Client in VMware vSphere Hypervisor (aka ESXi) 5.5 and 6.0 allows remote authenticated users to inject arbitrary web script or HTML via a crafted VM. **REFERENCE: CVE-2016-7463**	http://www.vmware.com/security/advisories/VMSA-2016-0023.html	O-VMW-ESXI-030116/183

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10