Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Application (A)					
7-zip					
P7zip P7zip is the Unix command-line port of 7-Zip, a file archiver that handles the 7z format which features very high compression ratios.					
Denial of Service	11/11/2016	5	A null pointer dereference bug affects the 16.02 and many old versions of p7zip. A lack of null pointer check for the variable folders.PackPositions in function CInArchive::ReadAndDecodePackedStreams in CPP/7zip/Archive/7z/7zIn.cpp, as used in the 7z.so library and in 7z applications, will cause a crash and a denial of service when decoding malformed 7z files. **Reference: CVE-2016-9296**	NA	A-7Z-P7ZIP-181116/01
Adobe					
Acrobat; Acrobat Dc; Acrobat Reader Dc; Reader The Adobe Acrobat and its versions are used for manipulating PDF files.					
Denial of Service; Execute Code; Overflow; Memory Corruption	10/11/2016	10	Adobe Reader and Acrobat before 11.0.18, Acrobat and Acrobat Reader DC Classic before 15.006.30243, and Acrobat and Acrobat	https://helpx.adobe.com/security/products/acrobat/apsb16-33.html	A-ADO-ACROB--181116/02

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

			Reader DC Continuous before 15.020.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors. **Reference: CVE-2016-4095**		
Connect Adobe Connect web conferencing software service offers immersive online meeting experiences for collaboration, virtual classrooms and large scale webinars.					
Cross Site Scripting	08/11/2016	4.3	Adobe Connect version 9.5.6 and earlier does not adequately validate input in the events registration module. This vulnerability could be exploited in cross-site scripting attacks. **Reference: CVE-2016-7851**	https://helpx.adobe.com/security/products/connect/apsb16-35.html	A-ADO-CONNE--181116/03
Flash Player Adobe Flash Player is freeware software for using content created on the Adobe Flash platform, including viewing multimedia, executing rich Internet applications, and streaming video and audio.					
Execute Code	01/11/2016	10	Use-after-free vulnerability in Adobe Flash Player before 23.0.0.205 on Windows and OS X and before 11.2.202.643 on Linux allows remote attackers to execute arbitrary code via unspecified vectors, as exploited in the wild in October 2016.	https://helpx.adobe.com/security/products/flash-player/apsb16-36.html	A-ADO-FLASH--181116/04

			Reference: CVE-2016-7855		
Flash Player; Flash Player For Linux Adobe Flash Player is freeware software for using content created on the Adobe Flash platform, including viewing multimedia, executing rich Internet applications, and streaming video and audio; Flash Player is also available for the Linux OS platform.					
Execute Code	08/11/2016	10	Adobe Flash Player versions 23.0.0.205 and earlier, 11.2.202.643 and earlier have an exploitable type confusion vulnerability. Successful exploitation could lead to arbitrary code execution. **Reference: CVE-2016-7865**	https://helpx.adobe.com/security/products/flash-player/apsb16-37.html	A-ADO-FLASH--181116/05
Execute Code	08/11/2016	10	Adobe Flash Player versions 23.0.0.205 and earlier, 11.2.202.643 and earlier have an exploitable use-after-free vulnerability. Successful exploitation could lead to arbitrary code execution. **Reference: CVE-2016-7864**	https://helpx.adobe.com/security/products/flash-player/apsb16-37.html	A-ADO-FLASH--181116/06
Execute Code	08/11/2016	10	Adobe Flash Player versions 23.0.0.205 and earlier, 11.2.202.643 and earlier have an exploitable use-after-free vulnerability. Successful exploitation could lead to arbitrary	https://helpx.adobe.com/security/products/flash-player/apsb16-37.html	A-ADO-FLASH--181116/07

			code execution. **Reference: CVE-2016-7863**		
Execute Code	08/11/2016	10	Adobe Flash Player versions 23.0.0.205 and earlier, 11.2.202.643 and earlier have an exploitable use-after-free vulnerability. Successful exploitation could lead to arbitrary code execution. **Reference: CVE-2016-7862**	https://helpx.adobe.com/security/products/flash-player/apsb16-37.html	A-ADO-FLASH--181116/08
Execute Code	08/11/2016	10	Adobe Flash Player versions 23.0.0.205 and earlier, 11.2.202.643 and earlier have an exploitable type confusion vulnerability. Successful exploitation could lead to arbitrary code execution. **Reference: CVE-2016-7861**	https://helpx.adobe.com/security/products/flash-player/apsb16-37.html	A-ADO-FLASH--181116/09
Execute Code	08/11/2016	10	Adobe Flash Player versions 23.0.0.205 and earlier, 11.2.202.643 and earlier have an exploitable type confusion vulnerability. Successful exploitation could lead to arbitrary code execution. **Reference: CVE-2016-7860**	https://helpx.adobe.com/security/products/flash-player/apsb16-37.html	A-ADO-FLASH--181116/10

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	08/11/2016	10	Adobe Flash Player versions 23.0.0.205 and earlier, 11.2.202.643 and earlier have an exploitable use-after-free vulnerability. Successful exploitation could lead to arbitrary code execution. **Reference: CVE-2016-7859**	https://helpx.adobe.com/security/products/flash-player/apsb16-37.html	A-ADO-FLASH--181116/11
Execute Code	08/11/2016	10	Adobe Flash Player versions 23.0.0.205 and earlier, 11.2.202.643 and earlier have an exploitable use-after-free vulnerability. Successful exploitation could lead to arbitrary code execution. **Reference: CVE-2016-7858**	https://helpx.adobe.com/security/products/flash-player/apsb16-37.html	A-ADO-FLASH--181116/12
Execute Code	08/11/2016	10	Adobe Flash Player versions 23.0.0.205 and earlier, 11.2.202.643 and earlier have an exploitable use-after-free vulnerability. Successful exploitation could lead to arbitrary code execution. **Reference: CVE-2016-7857**	https://helpx.adobe.com/security/products/flash-player/apsb16-37.html	A-ADO-FLASH--181116/13
Artifex					
Mujs MuJS is a lightweight implementation of the Javascript language in a library. Its primary purpose is					

to add scripting capability to other programs, but can also be used as an extensible scripting language.					
Denial of Service	11/11/2016	5	Artifex Software, Inc. MuJS before 5008105780c0b0182ea6eda83ad5598f225be3ee allows context-dependent attackers to conduct "denial of service (application crash)" attacks by using the "malformed labeled break/continue in JavaScript" approach, related to a "NULL pointer dereference" issue affecting the jscompile.c component. **Reference: CVE-2016-9294**	http://bugs.ghostscript.com/show_bug.cgi?id=697172	A-ART-MUJS--181116/14
Cisco					
Hosted Collaboration Mediation Fulfillment Cisco Hosted Collaboration Solution (HCS) is a next-generation unified communications and collaboration platform for service providers who want to offer unique Cisco collaboration technologies using hosted and managed models.					
Cross Site Request Forgery	03/11/2016	4.3	A cross-site request forgery (CSRF) vulnerability in the web interface of the Cisco Hosted Collaboration Mediation Fulfillment application could allow an unauthenticated, remote attacker to execute unwanted actions. More Information: CSCva54241. Known Affected	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161026-hcmf	A-CIS-HOSTE--181116/15

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

			Releases: 11.5(1). Known Fixed Releases: 11.5(0.98000.216). **Reference: CVE-2016-6454**		
Identity Services Engine Cisco Identity Services Engine (ISE) is a network administration product that enables the creation and enforcement of security and access policies for endpoint devices connected to the company's routers and switches. The purpose is to simplify identity management across diverse devices and applications.					
Execute Code; SQL Injection	03/11/2016	4.9	A vulnerability in the web framework code of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to execute arbitrary SQL commands on the database. More Information: CSCva46542. Known Affected Releases: 1.3(0.876). **Reference: CVE-2016-6453**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161026-ise	A-CIS-IDENT--181116/16
Ip Interoperability And Collaboration System Cisco IP Interoperability and Collaboration System (IPICS) can simplify radio dispatch operations and improve response to incidents, emergencies, and facility events.					
NA	03/11/2016	6.6	A vulnerability in the command-line interface of the Cisco IP Interoperability and Collaboration System (IPICS) could allow an authenticated, local attacker to elevate the privilege level associated with their session. More	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161026-ipics2	A-CIS-IPIN--181116/17

			Information: CSCva38636. Known Affected Releases: 4.10(1). Known Fixed Releases: 5.0(1). **Reference: CVE-2016-6430**		
Cross Site Scripting	03/11/2016	4.3	A vulnerability in the web framework code of the Cisco IP Interoperability and Collaboration System (IPICS) could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack. More Information: CSCva47092. Known Affected Releases: 4.10(1). **Reference: CVE-2016-6429**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161026-ipics1	A-CIS-IPIN--181116/18
Meeting App; Meeting Server Cisco WebEx video conferencing app helps you make decisions faster, with integrated audio, video and content sharing; Cisco Meeting Server brings premises-based video, audio, and web communication together to meet the collaboration needs of the modern workplace.					
Execute Code; Overflow	03/11/2016	7.5	A vulnerability in Cisco Meeting Server and Meeting App could allow an unauthenticated, remote attacker to execute arbitrary code on an affected system. This vulnerability affects the following products: Cisco Meeting Server releases prior to 2.0.1, Acano Server	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161102-cms	A-CIS-MEETI--181116/19

			releases prior to 1.8.16 and prior to 1.9.3, Cisco Meeting App releases prior to 1.9.8, Acano Meeting Apps releases prior to 1.8.35. More Information: CSCva75942 CSCvb67878. Known Affected Releases: 1.81.92.0. **Reference: CVE-2016-6447**		
Meeting Server Cisco Meeting Server brings premises-based video, audio, and web communication together to meet the collaboration needs of the modern workplace.					
Execute Code; Overflow	03/11/2016	7.5	Vulnerability in the Session Description Protocol (SDP) parser of Cisco Meeting Server could allow an unauthenticated, remote attacker to execute arbitrary code on an affected system. This vulnerability affects the following products: Cisco Meeting Server releases prior to Release 2.0.3, Acano Server releases 1.9.x prior to Release 1.9.5, Acano Server releases 1.8.x prior to Release 1.8.17. More Information: CSCva76004. Known Affected Releases: 1.8.x 1.92.0. **Reference: CVE-**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161102-cms1	A-CIS-MEETI--181116/20

			2016-6448		
Prime Collaboration Provisioning Prime Collaboration Provisioning provides features such as delegation to individual domains, template support for configuring infrastructure instances, advanced batch provisioning and so on.					
Cross Site Scripting	03/11/2016	4.3	Multiple vulnerabilities in the web framework code of the Cisco Prime Collaboration Provisioning could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against the user of the web interface of the affected system. More Information: CSCut43061 CSCut43066 CSCut43736 CSCut43738 CSCut43741 CSCut43745 CSCut43748 CSCut43751 CSCut43756 CSCut43759 CSCut43764 CSCut43766. Known Affected Releases: 10.6. **Reference: CVE-2016-6451**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161026-pcp	A-CIS-PRIME--181116/21
Prime Home Cisco Prime Home provides a feature-rich, standards-based remote management and provisioning solution that provides visibility into the home network, as also reducing operational costs and improving the subscriber experience.					
Bypass	03/11/2016	10	Vulnerability in the web-based graphical user interface (GUI) of Cisco Prime Home could allow an	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-	A-CIS-PRIME--181116/22

			unauthenticated, remote attacker to bypass authentication. The attacker could be granted full administrator privileges. Cisco Prime Home versions 5.1.1.6 and earlier and 5.2.2.2 and earlier have been confirmed to be vulnerable. Cisco Prime Home versions 6.0 and later are not vulnerable. More Information: CSCvb71732. Known Affected Releases: 5.0 5.0(1) 5.0(1.1) 5.0(1.2) 5.0(2) 5.15.1(0) 5.1(1) 5.1(1.3) 5.1(1.4) 5.1(1.5) 5.1(1.6) 5.1(2) 5.1(2.1) 5.1(2.3) 5.25.2(0.1) 5.2(1.0) 5.2(1.2) 5.2(2.0) 5.2(2.1) 5.2(2.2). **Reference: CVE-2016-6452**	20161102-cph	
Citrix					
Receiver Desktop Citrix Receiver is the easy-to-install client software that provides access to your XenDesktop and XenApp installations. With this free download you can access applications, desktops and data easily and securely from any device, including smartphones, tablets, PCs and Macs.					
Bypass	07/11/2016	4.6	Incorrect access control mechanisms in Citrix Receiver Desktop Lock 4.5 allow an attacker to bypass the authentication requirement by	NA	A-CIT-RECEI--181116/23

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

			leveraging physical access to a VDI for temporary disconnection of a LAN cable. **Reference: CVE-2016-9111**		
Dotcms					
Dotcms DotCMS is a free software/open source web content management system (WCM) for building/managing websites, content and content driven web applications.					
			SQL injection vulnerability in the "Site Browser > HTML pages" screen in dotCMS before 3.3.1 allows remote authenticated attackers to execute arbitrary SQL commands via the orderby parameter. **Reference: CVE-2016-8908**	NA	A-DOT-DOTCM--181116/24
Execute Code; SQL Injection	14/11/2016	6.5	SQL injection vulnerability in the "Content Types > Content Types" screen in dotCMS before 3.3.1 allows remote authenticated attackers to execute arbitrary SQL commands via the orderby parameter. **Reference: CVE-2016-8907**	NA	A-DOT-DOTCM--181116/25
Execute Code; SQL Injection	14/11/2016	6.5	SQL injection vulnerability in the "Site Browser > Links pages" screen in dotCMS before 3.3.1 allows remote authenticated attackers to execute	NA	A-DOT-DOTCM--181116/26

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

			arbitrary SQL commands via the orderby parameter. **Reference: CVE-2016-8906**		
Execute Code; SQL Injection	14/11/2016	6.5	SQL injection vulnerability in the JSONTags servlet in dotCMS before 3.3.1 allows remote authenticated attackers to execute arbitrary SQL commands via the sort parameter. **Reference: CVE-2016-8905**	NA	A-DOT-DOTCM--181116/27
Execute Code; SQL Injection	14/11/2016	6.5	SQL injection vulnerability in the "Site Browser > Containers pages" screen in dotCMS before 3.3.1 allows remote authenticated attackers to execute arbitrary SQL commands via the orderby parameter. **Reference: CVE-2016-8904**	NA	A-DOT-DOTCM--181116/28
Execute Code; SQL Injection	14/11/2016	6.5	SQL injection vulnerability in the "Site Browser > Templates pages" screen in dotCMS before 3.3.1 allows remote authenticated attackers to execute arbitrary SQL commands via the orderby parameter. **Reference: CVE-2016-8903**	NA	A-DOT-DOTCM--181116/29
Execute Code; SQL Injection	14/11/2016	7.5	SQL injection vulnerability in the	NA	A-DOT-DOTCM--

			categoriesServlet servlet in dotCMS before 3.3.1 allows remote not authenticated attackers to execute arbitrary SQL commands via the sort parameter. **Reference: CVE-2016-8902**		181116/30
EMC					
Avamar Data Store; Avamar Server Virtual Edition EMC Avamar Data Store is the easiest and fastest way to deploy a physical Avamar server. It combines Dell EMC certified hardware and Avamar backup and recovery software in a fully integrated, scalable, pre-packaged solution. It eliminates the hassles and complexity of working with multiple vendors for hardware, software, and support; Avamar Virtual Edition (AVE) uses Avamar data protection technology to protect VMware environments.					
NA	15/11/2016	7.2	EMC Avamar Data Store (ADS) and Avamar Virtual Edition (AVE) versions 7.3 and older contain a vulnerability that may expose the Avamar servers to potentially be compromised by malicious users. **Reference: CVE-2016-0909**	http://www.securityfocus.com/archive/1/539613	A-EMC-AVAMA--181116/31
Exponentcms					
Exponent Cms Exponent CMS is an Open Source Content Management System, based on PHP, MySQL and the Exponent Framework.					
SQL Injection	03/11/2016	5	Exponent CMS 2.3.9 suffers from a SQL injection vulnerability in "/framework/modules/help/controllers/helpController.php" affecting the version parameter. Impact is Information	https://github.com/exponentcms/exponent-cms/commit/d5c3c175b60bd26b2b74ec85b8f0d2544db2c8db	A-EXP-EXPON--181116/32

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

			Disclosure. **Reference: CVE-2016-9135**		
SQL Injection	03/11/2016	5	Exponent CMS 2.3.9 suffers from a SQL injection vulnerability in "/expPaginator.php" affecting the order parameter. Impact is Information Disclosure. **Reference: CVE-2016-9134**	https://github.com/exponentcms/exponent-cms/commit/d5c3c175b60bd26b2b74ec85b8f0d2544db2c8db	A-EXP-EXPON--181116/33
SQL Injection	03/11/2016	7.5	The Pixidou Image Editor in Exponent CMS prior to v2.3.9 patch 2 could be used to perform an fid SQL Injection. **Reference: CVE-2016-7453**	https://github.com/exponentcms/exponent-cms/commit/c1092f167cc6c78dc8bf9bf149946c5219413df3	A-EXP-EXPON--181116/34
Dirctory Traversal	03/11/2016	5	The Pixidou Image Editor in Exponent CMS prior to v2.3.9 patch 2 could be used to upload a malicious file to any folder on the site via a cpi directory traversal. **Reference: CVE-2016-7452**	https://github.com/exponentcms/exponent-cms/commit/c1092f167cc6c78dc8bf9bf149946c5219413df3	A-EXP-EXPON--181116/35
NA	03/11/2016	7.5	Exponent CMS before 2.3.9 is vulnerable to an attacker uploading a malicious script file using redirection to place the script in an unprotected folder, one allowing script execution. **Reference: CVE-2016-7095**	http://www.exponentcms.org/news/security-vulnerability-all-exponent-versions-june-2016	A-EXP-EXPON--181116/36
SQL Injection	04/11/2016	5	In /framework/modules	https://github.com/exponentcms	A-EXP-EXPON--

			/core/controllers/expHTMLEditorController.php of Exponent CMS 2.4.0, untrusted input is used to construct a table name, and in the selectObject method in mysqli class, table names are wrapped with a character that common filters do not filter, allowing for SQL Injection. Impact is Information Disclosure. **Reference: CVE-2016-9184**	/exponent-cms/commit/0ce8b94d745b818bd207933d9a2e7f32587c2c89	181116/37
SQL Injection; Bypass; Gain Information	04/11/2016	5	In /framework/modules/ecommerce/controllers/orderController.php of Exponent CMS 2.4.0, untrusted input is passed into selectObjectsBySql. The method selectObjectsBySql of class mysqli_database uses the injectProof method to prevent SQL injection, but this filter can be bypassed easily: it only sanitizes user input if there are odd numbers of ' or " characters. Impact is Information Disclosure. **Reference: CVE-2016-9183**	https://github.com/exponentcms/exponent-cms/commit/3b3557e9f6ba193a4c23c8ce5498fa285dddf3f3	A-EXP-EXPON--181116/38
Bypass	04/11/2016	5	Exponent CMS 2.4 uses PHP reflection to call a method of a controller class, and	https://github.com/exponentcms/exponent-cms/commit/68	A-EXP-EXPON--181116/39

			then uses the method name to check user permission. But, the method name in PHP reflection is case insensitive, and Exponent CMS permits undefined actions to execute by default, so an attacker can use a capitalized method name to bypass the permission check, e.g., controller=expHTMLEditor&action=preview&editor=ckeditor and controller=expHTMLEditor&action=Preview&editor=ckeditor. An anonymous user will be rejected for the former but can access the latter. **Reference: CVE-2016-9182**	4d79424f768db8bb345d5c68aa2a886239492b	
Execute Code; SQL Injection	07/11/2016	6.5	Multiple SQL injection vulnerabilities in the update method in framework/modules/core/controllers/expRatingController.php in Exponent CMS 2.4.0 allow remote authenticated users to execute arbitrary SQL commands via the (1) content_type or (2) subtype parameter. **Reference: CVE-2016-9242**	https://github.com/exponentcms/exponent-cms/commit/6172f67620ac13fc2f4e9d650c61937d48e9ecb9	A-EXP-EXPON--181116/40
SQL Injection	11/11/2016	7.5	In framework/modules/navigation/controller	https://github.com/exponentcms/exponent-	A-EXP-EXPON--181116/41

			s/navigationController.php in Exponent CMS v2.4.0 or older, the parameter "target" of function "DragnDropReRank" is directly used without any filtration which caused SQL injection. The payload can be used like this: /navigation/DragnDropReRank/target/1. **Reference: CVE-2016-9288**	cms/commit/2dffb2e7eafe4830e3483a4b437873022c461ba	
Gain Information	11/11/2016	5	framework/modules/users/controllers/usersController.php in Exponent CMS v2.4.0patch1 does not properly restrict access to user records, which allows remote attackers to read address information, as demonstrated by an address/show/id/1 URI. **Reference: CVE-2016-9286**	https://github.com/exponentcms/exponent-cms/commit/e38aae66c785f08f3907aa121378caf71ca5f2d7	A-EXP-EXPON--181116/42
Gain Information	11/11/2016	5	framework/modules/addressbook/controllers/addressController.php in Exponent CMS v2.4.0 allows remote attackers to read user information via a modified id number, as demonstrated by address/edit/id/1, related to an "addresses, countries, and regions" issue. **Reference: CVE-**	https://github.com/exponentcms/exponent-cms/commit/9eed1e82fb9e6d0d41e7dd10672df48045a9b59	A-EXP-EXPON--181116/43

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

			2016-9285		
Gain Information	11/11/2016	5	getUsersByJSON in framework/modules/users/controllers/usersController.php in Exponent CMS v2.4.0 allows remote attackers to read user information via users/getUsersByJSON/sort/ and a trailing string. **Reference: CVE-2016-9284**	https://github.com/exponentcms/exponent-cms/commit/e7b6856ac384bf2b8ea7761a1e46d6e4186d36f4	A-EXP-EXPON--181116/44
SQL Injection	11/11/2016	5	SQL Injection in framework/core/subsystems/expRouter.php in Exponent CMS v2.4.0 allows remote attackers to read database information via address/addContentToSearch/id/ and a trailing string, related to a "sef URL" issue. **Reference: CVE-2016-9283**	https://github.com/exponentcms/exponent-cms/commit/559792be727f4e731bfcb3935f5beec7749e9ce9	A-EXP-EXPON--181116/45
SQL Injection	11/11/2016	5	SQL Injection in framework/modules/search/controllers/searchController.php in Exponent CMS v2.4.0 allows remote attackers to read database information via action=search&module=search with the search_string parameter. **Reference: CVE-2016-9282**	https://github.com/exponentcms/exponent-cms/commit/e83721a5b9fcc88e1141a8fb29c3d1bd522257c1	A-EXP-EXPON--181116/46
Denial of Service; SQL	11/11/2016	6.4	A Blind SQL Injection Vulnerability in	https://exponentcms.lighthouseap	A-EXP-EXPON--

Injection			Exponent CMS through 2.4.0, with the rerank array parameter, can lead to site database information disclosure and denial of service. **Reference: CVE-2016-9272**	p.com/projects/61783/tickets/1394-blind-sql-injection-vulnerability-in-exponent-cms-240-4	181116/47
SQL Injection	15/11/2016	7.5	In /framework/modules/notfound/controllers/notfoundController.php of Exponent CMS 2.4.0 patch1, untrusted input is passed into getSearchResults. The method getSearchResults is defined in the search model with the parameter '$term' used directly in SQL. Impact is a SQL injection. **Reference: CVE-2016-9287**	https://github.com/exponentcms/exponent-cms/commit/4327ea96b3de89440693e06d03038121aa1fdcea	A-EXP-EXPON--181116/48
Git For Windows Project					
Git For Windows Git for Windows focuses on offering a lightweight, native set of tools that bring the full feature set of the Git SCM to Windows while providing appropriate user interfaces for experienced Git users and novices alike.					
Gain Privileges	11/11/2016	4.4	Untrusted search path vulnerability in Git 1.x for Windows allows local users to gain privileges via a Trojan horse git.exe file in the current working directory. NOTE: 2.x is unaffected. **Reference: CVE-2016-9274**	NA	A-GIT-GITF--181116/49

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

Gitlab					
Gitlab Gitlab is a free software, which provides Git repository management, code reviews, issue tracking, activity feeds and wikis.					
Gain Information	03/11/2016	4	GitLab versions 8.9.x and above contain a critical security flaw in the "import/export project" feature of GitLab. Added in GitLab 8.9, this feature allows a user to export and then re-import their projects as tape archive files (tar). All GitLab versions prior to 8.13.0 restricted this feature to administrators only. Starting with version 8.13.0 this feature was made available to all users. This feature did not properly check for symbolic links in user-provided archives and therefore it was possible for an authenticated user to retrieve the contents of any file accessible to the GitLab service account. This included sensitive files such as those that contain secret tokens used by the GitLab service to authenticate users.	https://about.gitlab.com/2016/11/02/cve-2016-9086-patches/	A-GIT-GITLA--181116/50

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

			GitLab CE and EE versions 8.13.0 through 8.13.2, 8.12.0 through 8.12.7, 8.11.0 through 8.11.10, 8.10.0 through 8.10.12, and 8.9.0 through 8.9.11 are affected. **Reference: CVE-2016-9086**		
ISC					
Bind BIND is open source software that implements the Domain Name System (DNS) protocols for the Internet.					
Denial of Service	02/11/2016	5	named in ISC BIND 9.x before 9.9.9-P4, 9.10.x before 9.10.4-P4, and 9.11.x before 9.11.0-P1 allows remote attackers to cause a denial of service (assertion failure and daemon exit) via a DNAME record in the answer section of a response to a recursive query, related to db.c and resolver.c. **Reference: CVE-2016-8864**	https://kb.isc.org/article/AA-01434	A-ISC-BIND--181116/51
Joomla					
Joomla! Joomla! is the mobile-ready and user-friendly way to build your website. It is free and open source.					
NA	04/11/2016	6.8	The register method in the UsersModelRegistration class in controllers/user.php in the Users component in	https://github.com/joomla/joomla-cms/commit/bae1d43938c878480cfd73671e4945211538fdcf	A-JOO-JOOML--181116/52

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

			Joomla! before 3.6.4, when registration has been disabled, allows remote attackers to create user accounts by leveraging failure to check the Allow User Registration configuration setting. **Reference: CVE-2016-8870**		
Gain Privileges	04/11/2016	7.5	The register method in the UsersModelRegistration class in controllers/user.php in the Users component in Joomla! before 3.6.4 allows remote attackers to gain privileges by leveraging incorrect use of unfiltered data when registering on a site. **Reference: CVE-2016-8869**	https://github.com/joomla/joomla-cms/commit/bae1d43938c878480cfd73671e4945211538fdcf	A-JOO-JOOML--181116/53
Microfocus					
Rumba RUMBA software makes it easy to connect to and use information on IBM mainframe, IBM iSeries (AS/400), UNIX, Hewlett-Packard, and VAX systems. Micro Focuss modular-based products ensure optimal performance and fast, flexible custom application development.					
Execute Code; Overflow	03/11/2016	7.5	Stack buffer overflow in the send.exe and receive.exe components of Micro Focus Rumba 9.4 and earlier could be used by local attackers or attackers able to	https://www.exploit-db.com/exploits/40648/	A-MIC-RUMBA--181116/54

			inject arguments to these binaries to execute code. **Reference: CVE-2016-9176**		
Microsoft					
Edge Edge is a smaller, more streamlined browser built on Web standards and designed for Web services.					
Denial of Service; Execute Code; Overflow; Memory Corruption	10/11/2016	7.6	The Chakra JavaScript scripting engine in Microsoft Edge allows 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-2016-7200, CVE-2016-7201, CVE-2016-7202, CVE-2016-7203, CVE-2016-7208, CVE-2016-7240, and CVE-2016-7242. **Reference: CVE-2016-7243**	http://technet.microsoft.com/en-us/security/bulletin/ms16-129	A-MIC-EDGE--181116/55
Denial of Service; Execute Code; Overflow; Memory Corruption	10/11/2016	7.6	The Chakra JavaScript scripting engine in Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine	http://technet.microsoft.com/en-us/security/bulletin/ms16-129	A-MIC-EDGE--181116/56

			Memory Corruption Vulnerability," a different vulnerability than CVE-2016-7200, CVE-2016-7201, CVE-2016-7202, CVE-2016-7203, CVE-2016-7208, CVE-2016-7240, and CVE-2016-7243. **Reference: CVE-2016-7242**		
Denial of Service; Execute Code; Overflow; Memory Corruption	10/11/2016	7.6	The Chakra JavaScript scripting engine in Microsoft Edge allows 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-2016-7200, CVE-2016-7201, CVE-2016-7202, CVE-2016-7203, CVE-2016-7208, CVE-2016-7242, and CVE-2016-7243. **Reference: CVE-2016-7240**	http://technet.microsoft.com/en-us/security/bulletin/ms16-129	A-MIC-EDGE--181116/57
NA	10/11/2016	2.6	Microsoft Edge allows remote attackers to spoof web content via a crafted web site, aka "Microsoft Edge Spoofing	http://technet.microsoft.com/en-us/security/bulletin/ms16-129	A-MIC-EDGE--181116/58

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

			Vulnerability." **Reference: CVE-2016-7209**		
Denial of Service; Execute Code; Overflow; Memory Corruption	10/11/2016	7.6	The Chakra JavaScript scripting engine in Microsoft Edge allows 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-2016-7200, CVE-2016-7201, CVE-2016-7202, CVE-2016-7203, CVE-2016-7240, CVE-2016-7242, and CVE-2016-7243. **Reference: CVE-2016-7208**	http://technet.microsoft.com/en-us/security/bulletin/ms16-129	A-MIC-EDGE--181116/59
Gain Information	10/11/2016	2.6	Microsoft Edge allows remote attackers to access arbitrary "My Documents" files via a crafted web site, aka "Microsoft Edge Information Disclosure Vulnerability." **Reference: CVE-2016-7204**	http://technet.microsoft.com/en-us/security/bulletin/ms16-129	A-MIC-EDGE--181116/60
Denial of Service; Execute Code; Overflow; Memory Corruption	10/11/2016	7.6	The Chakra JavaScript scripting engine in Microsoft Edge allows remote attackers to execute	http://technet.microsoft.com/en-us/security/bulletin/ms16-129	A-MIC-EDGE--181116/61

			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-2016-7200, CVE-2016-7201, CVE-2016-7202, CVE-2016-7208, CVE-2016-7240, CVE-2016-7242, and CVE-2016-7243. **Reference: CVE-2016-7203**		
Denial of Service; Execute Code; Overflow; Memory Corruption	10/11/2016	7.6	The Chakra JavaScript scripting engine in Microsoft Edge allows 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-2016-7200, CVE-2016-7201, CVE-2016-7203, CVE-2016-7208, CVE-2016-7240, CVE-2016-7242, and CVE-2016-7243. **Reference: CVE-2016-7202**	http://technet.microsoft.com/en-us/security/bulletin/ms16-129	A-MIC-EDGE--181116/62

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	10/11/2016	7.6	The Chakra JavaScript scripting engine in Microsoft Edge allows 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-2016-7200, CVE-2016-7202, CVE-2016-7203, CVE-2016-7208, CVE-2016-7240, CVE-2016-7242, and CVE-2016-7243. **Reference: CVE-2016-7201**	http://technet.microsoft.com/en-us/security/bulletin/ms16-129	A-MIC-EDGE--181116/63
Denial of Service; Execute Code; Overflow; Memory Corruption	10/11/2016	7.6	The Chakra JavaScript scripting engine in Microsoft Edge allows 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-2016-7201, CVE-2016-7202, CVE-2016-7203, CVE-2016-7208, CVE-2016-7240, CVE-2016-7242,	http://technet.microsoft.com/en-us/security/bulletin/ms16-129	A-MIC-EDGE--181116/64

			and CVE-2016-7243. **Reference: CVE-2016-7200**		
Edge; Internet Explorer Edge is a smaller, more streamlined browser built on Web standards and designed for Web services; Internet Explorer is a web browser developed by Microsoft and included as part of the Microsoft Windows line of operating systems.					
Bypass; Gain Information	10/11/2016	2.6	Microsoft Internet Explorer 9 through 11 and Microsoft Edge allow remote attackers to bypass the Same Origin Policy and obtain sensitive window-state information via a crafted web site, aka "Microsoft Browser Information Disclosure Vulnerability." **Reference: CVE-2016-7199**	NA	A-MIC-EDGE;--181116/65
Denial of Service; Execute Code; Overflow; Memory Corruption	10/11/2016	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," a different vulnerability than CVE-2016-7195. **Reference: CVE-2016-7198**	NA	A-MIC-EDGE;--181116/66
Denial of Service; Execute	10/11/2016	7.6	Microsoft Internet Explorer 10 and 11	NA	A-MIC-EDGE--

Code; Overflow; Memory Corruption			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-2016-7196**		181116/67
Denial of Service; Execute Code; Overflow; Memory Corruption	10/11/2016	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," a different vulnerability than CVE-2016-7198. **Reference: CVE-2016-7195**	NA	A-MIC-EDGE;--181116/68
Excel For Mac; Office; Office Compatibility Pack; Office Web Apps; Sharepoint Server; Word; Word Automation Services; Word For Mac; Word Viewer; Powerpoint; Powerpoint Viewer MS Office offers various applications like Word, Excel, Powerpoint, etc for the PC and mobile platforms; Microsoft Excel is a spreadsheet developed by Microsoft for Windows, macOS, Android and iOS. It features calculation, graphing tools, pivot tables, and a macro programming language called Visual Basic for Applications.					
Denial of Service; Gain Information	10/11/2016	4.3	Microsoft Word 2007, Office 2010 SP2, Word 2010 SP2, Word for Mac 2011, Excel for Mac 2011, Word Viewer, Office Compatibility Pack SP3, Word	http://technet.microsoft.com/en-us/security/bulletin/ms16-133	A-MIC-EXCEL--181116/69

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

			Automation Services on SharePoint Server 2013 SP1, 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 Office document, aka "Microsoft Office Information Disclosure Vulnerability." **Reference: CVE-2016-7233**		
Execute Code; Overflow; Memory Corruption	10/11/2016	9.3	Microsoft Word 2007, Office 2010 SP2, Word 2010 SP2, Word 2013 SP1, Word 2013 RT SP1, Word for Mac 2011, Excel for Mac 2011, Word 2016 for Mac, Office Compatibility Pack SP3, Word Automation Services on SharePoint Server 2010 SP2, Word Automation Services on SharePoint Server 2013 SP1, Office Web Apps 2010 SP2, and Office Web Apps Server 2013 SP1 allow remote attackers to execute arbitrary code via a crafted Office	http://technet.microsoft.com/en-us/security/bulletin/ms16-133	A-MIC-EXCEL--181116/70

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

			document, aka "Microsoft Office Memory Corruption Vulnerability." **Reference: CVE-2016-7234**		
Execute Code; Overflow; Memory Corruption	10/11/2016	9.3	Microsoft Word 2007, Office 2010 SP2, Word 2010 SP2, Word for Mac 2011, Excel for Mac 2011, and Office Compatibility Pack SP3 allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability." **Reference: CVE-2016-7235**	http://technet.microsoft.com/en-us/security/bulletin/ms16-133	A-MIC-EXCEL--181116/71
Execute Code; Overflow; Memory Corruption	10/11/2016	9.3	Microsoft Excel 2007 SP3, Excel for Mac 2011, Office Compatibility Pack SP3, and Excel Viewer allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability." **Reference: CVE-2016-7231**	http://technet.microsoft.com/en-us/security/bulletin/ms16-133	A-MIC-EXCEL--181116/72
Execute Code; Overflow; Memory Corruption	10/11/2016	9.3	Microsoft Excel 2007 SP3, Excel 2010 SP2, Excel 2013 SP1, Excel 2013 RT SP1, Excel 2016, Excel for Mac	http://technet.microsoft.com/en-us/security/bulletin/ms16-133	A-MIC-EXCEL--181116/73

			2011, Excel 2016 for Mac, Office Compatibility Pack SP3, and Excel Viewer allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability." **Reference: CVE-2016-7229**		
Execute Code; Overflow; Memory Corruption	10/11/2016	9.3	Microsoft Excel 2007 SP3, Excel 2010 SP2, Excel 2013 SP1, Excel 2013 RT SP1, Excel 2016, Excel for Mac 2011, Excel 2016 for Mac, and Office Compatibility Pack SP3 allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability." **Reference: CVE-2016-7228**	http://technet.microsoft.com/en-us/security/bulletin/ms16-133	A-MIC-EXCEL--181116/74
Execute Code; Overflow; Memory Corruption	10/11/2016	9.3	Microsoft Excel 2007 SP3, Excel 2010 SP2, Excel 2013 SP1, Excel 2013 RT SP1, Excel 2016, Excel for Mac 2011, Excel 2016 for Mac, and Office Compatibility Pack SP3 allow remote attackers to execute arbitrary code via a	http://technet.microsoft.com/en-us/security/bulletin/ms16-133	A-MIC-EXCEL--181116/75

			crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability." **Reference: CVE-2016-7213**		
Execute Code; Overflow; Memory Corruption	10/11/2016	9.3	Microsoft Excel 2010 SP2, Excel for Mac 2011, Excel 2016 for Mac, and Excel Services on SharePoint Server 2010 SP2 allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability." **Reference: CVE-2016-7236**	http://technet.microsoft.com/en-us/security/bulletin/ms16-133	A-MIC-EXCEL--181116/76
Execute Code; Overflow; Memory Corruption	10/11/2016	9.3	Microsoft Office 2007 SP3, Office 2010 SP2, Office 2013 SP1, Office 2013 RT SP1, and Office 2016 allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability." **Reference: CVE-2016-7245**	http://technet.microsoft.com/en-us/security/bulletin/ms16-133	A-MIC-OFFIC--181116/77
Denial of Service	10/11/2016	4.3	Microsoft Office 2007 SP3 allows remote attackers to cause a denial of service (application	http://technet.microsoft.com/en-us/security/bulletin/ms16-133	A-MIC-OFFIC--181116/78

			hang) via a crafted Office document, aka "Microsoft Office Denial of Service Vulnerability." **Reference: CVE-2016-7244**		
Execute Code; Overflow; Memory Corruption	10/11/2016	9.3	Microsoft PowerPoint 2010 SP2, PowerPoint Viewer, and Office Web Apps 2010 SP2 allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability." **Reference: CVE-2016-7230**	http://technet.microsoft.com/en-us/security/bulletin/ms16-133	A-MIC-OFFIC--181116/79
Execute Code; Overflow; Memory Corruption	10/11/2016	9.3	Microsoft Word 2007, Office 2010 SP2, Word 2010 SP2, Word for Mac 2011, and Office Compatibility Pack SP3 allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability." **Reference: CVE-2016-7232**	http://technet.microsoft.com/en-us/security/bulletin/ms16-133	A-MIC-OFFIC--181116/80
SQL Server Microsoft SQL Server is a relational database management system developed by Microsoft. As a database server, it is a software product with the primary function of storing and retrieving data as requested by other software applications, which may run either on the same computer or on another computer across a network (including the Internet).					
Gain Privileges	10/11/2016	6.5	Microsoft SQL	http://technet.m	A-MIC-SQL

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

			Server 2014 SP1, 2014 SP2, and 2016 does not properly perform a cast of an unspecified pointer, which allows remote authenticated users to gain privileges via unknown vectors, aka "SQL RDBMS Engine Elevation of Privilege Vulnerability." **Reference: CVE-2016-7250**	icrosoft.com/en-us/security/bulletin/ms16-136	S--181116/81
Gain Privileges	10/11/2016	6.5	Microsoft SQL Server 2016 does not properly perform a cast of an unspecified pointer, which allows remote authenticated users to gain privileges via unknown vectors, aka "SQL RDBMS Engine Elevation of Privilege Vulnerability." **Reference: CVE-2016-7249**	http://technet.microsoft.com/en-us/security/bulletin/ms16-136	A-MIC-SQLS--181116/82
Moinmo					
Moinmoin MoinMoin is a wiki engine implemented in Python, initially based on the PikiPiki wiki engine. Its name is a play on the North German greeting Moin, repeated as in WikiWiki.					
Cross Site Scripting	10/11/2016	4.3	MoinMoin 1.9.8 allows remote attackers to conduct "JavaScript injection" attacks by using the "page creation" approach, related to a "Cross Site Scripting (XSS)"	https://www.curesec.com/blog/article/blog/MoinMoin-198-XSS-175.html	A-MOI-MOINM--181116/83

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

			issue affecting the action=AttachFile (via page name) component. **Reference: CVE-2016-7148**		
Cross Site Scripting	10/11/2016	4.3	MoinMoin 1.9.8 allows remote attackers to conduct "JavaScript injection" attacks by using the "page creation or crafted URL" approach, related to a "Cross Site Scripting (XSS)" issue affecting the action=fckdialog&dialog=attachment (via page name) component. **Reference: CVE-2016-7146**	https://www.curesec.com/blog/article/blog/MoinMoin-198-XSS-175.html	A-MOI-MOINM--181116/84
Moodle					
Moodle Moodle is free and open-source software learning management system written in PHP and distributed under the GNU General Public License.					
Cross Site Scripting	04/11/2016	4.3	Cross-site scripting (XSS) vulnerabilities in Moodle CMS on or before 3.1.2 allow remote attackers to inject arbitrary web script or HTML via the s_additionalhtmlhead, s_additionalhtmltopofbody, and s_additionalhtmlfooter parameters. **Reference: CVE-2016-9188**	https://packetstormsecurity.com/files/139466/Moodle-CMS-3.1.2-Cross-Site-Scripting-File-Upload.html	A-MOO-MOODL--181116/85
Execute Code	04/11/2016	6.5	Unrestricted file upload vulnerability	https://packetstormsecurity.com	A-MOO-MOODL--

			in the double extension support in the "image" module in Moodle 3.1.2 allows remote authenticated users to execute arbitrary code by uploading a file with an executable extension, and then accessing it via unspecified vectors. **Reference: CVE-2016-9187**	/files/139466/Moodle-CMS-3.1.2-Cross-Site-Scripting-File-Upload.html	181116/86
Execute Code	04/11/2016	6.5	Unrestricted file upload vulnerability in the "legacy course files" and "file manager" modules in Moodle 3.1.2 allows remote authenticated users to execute arbitrary code by uploading a file with an executable extension, and then accessing it via unspecified vectors. **Reference: CVE-2016-9186**	https://packetstormsecurity.com/files/139466/Moodle-CMS-3.1.2-Cross-Site-Scripting-File-Upload.html	A-MOO-MOODL--181116/87
Novell					
Open Enterprise Server 11; Open Enterprise Server 2015 Open Enterprise Server brings the industry's most advanced file and print services onto the latest SUSE Linux Enterprise platform.					
NA	15/11/2016	6.4	Vulnerability in Novell Open Enterprise Server (OES2015 SP1 before Scheduled Maintenance Update 10992, OES2015 before Scheduled Maintenance Update	http://download.novell.com/Download?buildid=s9_RxhgC8KU~	A-NOV-OPEN --181116/88

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

			10990, OES11 SP3 before Scheduled Maintenance Update 10991, OES11 SP2 before Scheduled Maintenance Update 10989) might allow authenticated remote attackers to perform unauthorized file access and modification. **Reference: CVE-2016-5763**		
Nvidia					
Geforce Experience NA					
Denial of Service; Overflow	08/11/2016	7.2	For the NVIDIA Quadro, NVS, and GeForce products, NVIDIA GeForce Experience R340 before GFE 2.11.4.125 and R375 before GFE 3.1.0.52 contains a vulnerability in the kernel mode layer (nvstreamkms.sys) allowing a user to cause a stack buffer overflow with specially crafted executable paths, leading to a denial of service or escalation of privileges. **Reference: CVE-2016-8812**	http://nvidia.custhelp.com/app/answers/detail/a_id/4247	A-NVI-GEFOR--181116/89
Execute Code	08/11/2016	7.2	For the NVIDIA Quadro, NVS, and GeForce products, GFE GameStream	http://nvidia.custhelp.com/app/answers/detail/a_id/4213	A-NVI-GEFOR--181116/90

			and NVTray Plugin unquoted service path vulnerabilities are examples of the unquoted service path vulnerability in Windows. A successful exploit of a vulnerable service installation can enable malicious code to execute on the system at the system/user privilege level. The CVE-2016-5852 ID is for the NVTray Plugin unquoted service path. **Reference: CVE-2016-5852**		
Denial of Service	08/11/2016	4.9	For the NVIDIA Quadro, NVS, and GeForce products, improper sanitization of parameters in the NVStreamKMS.sys API layer caused a denial of service vulnerability (blue screen crash) within the NVIDIA Windows graphics drivers. **Reference: CVE-2016-4961**	http://nvidia.custhelp.com/app/answers/detail/a_id/4213	A-NVI-GEFOR--181116/91
NA	08/11/2016	6.9	For the NVIDIA Quadro, NVS, and GeForce products, the NVIDIA NVStreamKMS.sys service component is improperly validating user-supplied data	http://nvidia.custhelp.com/app/answers/detail/a_id/4213	A-NVI-GEFOR--181116/92

			through its API entry points causing an elevation of privilege. **Reference: CVE-2016-4960**		
Execute Code	08/11/2016	7.2	For the NVIDIA Quadro, NVS, and GeForce products, GFE GameStream and NVTray Plugin unquoted service path vulnerabilities are examples of the unquoted service path vulnerability in Windows. A successful exploit of a vulnerable service installation can enable malicious code to execute on the system at the system/user privilege level. The CVE-2016-3161 ID is for the GameStream unquoted service path. **Reference: CVE-2016-3161**	http://nvidia.custhelp.com/app/answers/detail/a_id/4213	A-NVI-GEFOR--181116/93
Gpu Driver Nvidia GPU-accelerated computing is the use of a graphics processing unit (GPU) together with a CPU to accelerate deep learning, analytics, and engineering applications.					
Denial of Service	08/11/2016	7.2	For the NVIDIA Quadro, NVS, and GeForce products, NVIDIA Windows GPU Display Driver R340 before 342.00 and R375 before 375.63 contains a vulnerability in the kernel mode layer	http://nvidia.custhelp.com/app/answers/detail/a_id/4247	A-NVI-GPUD--181116/94

			(nvlddmkm.sys) handler for DxgDdiEscape ID 0x7000170 where the size of an input buffer is not validated, leading to denial of service or potential escalation of privileges. **Reference: CVE-2016-8811**		
Denial of Service	08/11/2016	7.2	For the NVIDIA Quadro, NVS, and GeForce products, NVIDIA Windows GPU Display Driver R340 before 342.00 and R375 before 375.63 contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgDdiEscape ID 0x100009a where a value passed from an 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-2016-8810**	http://nvidia.custhelp.com/app/answers/detail/a_id/4247	A-NVI-GPUD--181116/95
Denial of Service	08/11/2016	7.2	For the NVIDIA Quadro, NVS, and GeForce products, NVIDIA Windows GPU Display Driver R340 before 342.00 and R375 before 375.63 contains a vulnerability in the	http://nvidia.custhelp.com/app/answers/detail/a_id/4247	A-NVI-GPUD--181116/96

			kernel mode layer (nvlddmkm.sys) handler for DxgDdiEscape ID 0x70001b2 where the size of an input buffer is not validated, leading to denial of service or potential escalation of privileges. **Reference: CVE-2016-8809**		
Denial of Service	08/11/2016	7.2	For the NVIDIA Quadro, NVS, and GeForce products, NVIDIA Windows GPU Display Driver R340 before 342.00 and R375 before 375.63 contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgDdiEscape ID 0x70000d5 where a value passed from an 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-2016-8808**	http://nvidia.custhelp.com/app/answers/detail/a_id/4247	A-NVI-GPUD--181116/97
Denial of Service; Overflow	08/11/2016	7.2	For the NVIDIA Quadro, NVS, and GeForce products, NVIDIA Windows GPU Display Driver R340 before 342.00 and R375 before 375.63 contains a	http://nvidia.custhelp.com/app/answers/detail/a_id/4247	A-NVI-GPUD--181116/98

			vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgDdiEscape ID 0x10000e9 where a value is passed from an user to the driver is used without validation as the size input to memcpy() causing a stack buffer overflow, leading to denial of service or potential escalation of privileges. **Reference: CVE-2016-8807**		
Denial of Service	08/11/2016	7.2	For the NVIDIA Quadro, NVS, and GeForce products, NVIDIA Windows GPU Display Driver R340 before 342.00 and R375 before 375.63 contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgDdiEscape ID 0x5000027 where a pointer passed from an user to the driver is used without validation, leading to denial of service or potential escalation of privileges. **Reference: CVE-2016-8806**	http://nvidia.custhelp.com/app/answers/detail/a_id/4247	A-NVI-GPUD--181116/99
Denial of Service	08/11/2016	7.2	For the NVIDIA Quadro, NVS, and GeForce products,	http://nvidia.custhelp.com/app/answers/detail/a_	A-NVI-GPUD--181116/100

			NVIDIA Windows GPU Display Driver R340 before 342.00 and R375 before 375.63 contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgDdiEscape ID 0x7000014 where a value passed from an 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-2016-8805**	id/4247	
Denial of Service	08/11/2016	7.2	For the NVIDIA Quadro, NVS, and GeForce products, NVIDIA Windows GPU Display Driver R340 before 342.00 and R375 before 375.63 contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgDdiEscape ID 0x100010b where a missing array bounds check can allow a user to write to kernel memory, leading to denial of service or potential escalation of privileges. **Reference: CVE-2016-7391**	http://nvidia.custhelp.com/app/answers/detail/a_id/4247	A-NVI-GPUD--181116/101

Denial of Service	08/11/2016	7.2	For the NVIDIA Quadro, NVS, and GeForce products, NVIDIA Windows GPU Display Driver R340 before 342.00 and R375 before 375.63 contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgDdiEscape ID 0x7000194 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-2016-7390**	http://nvidia.custhelp.com/app/answers/detail/a_id/4247	A-NVI-GPUD--181116/102
Gain Privileges	08/11/2016	7.2	For the NVIDIA Quadro, NVS, GeForce, and Tesla products, NVIDIA GPU Display Driver on Linux R304 before 304.132, R340 before 340.98, R367 before 367.55, R361_93 before 361.93.03, and R370 before 370.28 contains a vulnerability in the kernel mode layer (nvidia.ko) handler for mmap() where improper input validation may allow users to gain access to arbitrary	http://nvidia.custhelp.com/app/answers/detail/a_id/4246	A-NVI-GPUD--181116/103

			physical memory, leading to an escalation of privileges. **Reference: CVE-2016-7389**		
Denial of Service	08/11/2016	7.2	For the NVIDIA Quadro, NVS, and GeForce products, NVIDIA Windows GPU Display Driver R340 before 342.00 and R375 before 375.63 contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler where a NULL pointer dereference caused by invalid user input may lead to denial of service or potential escalation of privileges. **Reference: CVE-2016-7388**	http://nvidia.custhelp.com/app/answers/detail/a_id/4247	A-NVI-GPUD--181116/104
Denial of Service	08/11/2016	7.2	For the NVIDIA Quadro, NVS, and GeForce products, NVIDIA Windows GPU Display Driver R340 before 342.00 and R375 before 375.63 contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgDdiEscape ID 0x600000D where a value passed from a user to the driver is used without val **Reference: CVE-2016-7387**	http://nvidia.custhelp.com/app/answers/detail/a_id/4247	A-NVI-GPUD--181116/105

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	08/11/2016	6.1	For the NVIDIA Quadro, NVS, and GeForce products, improper sanitization of parameters in the NVAPI support layer causes a denial of service vulnerability (blue screen crash) within the NVIDIA Windows graphics drivers. **Reference: CVE-2016-5025**	http://nvidia.custhelp.com/app/answers/detail/a_id/4213	A-NVI-GPUD--181116/106
Denial of Service	08/11/2016	7.8	For the NVIDIA Quadro, NVS, and GeForce products, there is a Remote Desktop denial of service. A successful exploit of a vulnerable system will result in a kernel null pointer dereference, causing a blue screen crash. **Reference: CVE-2016-4959**	http://nvidia.custhelp.com/app/answers/detail/a_id/4213	A-NVI-GPUD--181116/107
Objective Development					
Little Snitch Little Snitch is a host-based application firewall for Mac OS X. It can be used to monitor applications, preventing or permitting them to connect to attached networks through advanced rules.					
Overflow	15/11/2016	7.2	Little Snitch version 3.0 through 3.6.1 suffer from a buffer overflow vulnerability that could be locally exploited which could lead to an escalation of privileges (EoP) and unauthorised ring0 access to the	https://speakerdeck.com/patrickwardle/defcon-2016-i-got-99-problems-but-little-snitch-aint-one	A-OBJ-LITTL--181116/108

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

			operating system. The buffer overflow is related to insufficient checking of parameters to the "OSMalloc" and "copyin" kernel API calls. **Reference: CVE-2016-8661**		
Openstack					
Heat Heat is the main project in the OpenStack Orchestration program. It implements an orchestration engine to launch multiple composite cloud applications based on templates in the form of text files that can be treated like code.					
Gain Information	04/11/2016	4	In OpenStack Heat, by launching a new Heat stack with a local URL an authenticated user may conduct network discovery revealing internal network configuration. Affected versions are <=5.0.3, >=6.0.0 <=6.1.0, and ==7.0.0. **Reference: CVE-2016-9185**	https://bugs.launchpad.net/ossa/+bug/1606500	A-OPE-HEAT--181116/109
Python					
Pillow: NA					
Execute Code	04/11/2016	6.8	Pillow before 3.3.2 allows context-dependent attackers to execute arbitrary code by using the "crafted image file" approach, related to an "Insecure Sign Extension" issue affecting the ImagingNew in Storage.c	https://github.com/python-pillow/Pillow/pull/2146/commits/5d8a0be45aad78c5a22c8d099118ee26ef8144af	A-PYT-PILLO--181116/110

			component. **Reference: CVE-2016-9190**		
Overflow; Gain Information	04/11/2016	4.3	Pillow before 3.3.2 allows context-dependent attackers to obtain sensitive information by using the "crafted image file" approach, related to an "Integer Overflow" issue affecting the Image.core.map_buffer in map.c component. **Reference: CVE-2016-9189**	http://pillow.readthedocs.io/en/3.4.x/releasenotes/3.3.2.html	A-PYT-PILLO--181116/111
Qemu					
Qemu QEMU supports virtualization when executing under the Xen hypervisor or using the KVM kernel module in Linux.					
Denial of Service	04/11/2016	1.9	The rtl8139_cplus_transmit function in hw/net/rtl8139.c in QEMU (aka Quick Emulator) allows local guest OS administrators to cause a denial of service (infinite loop and CPU consumption) by leveraging failure to limit the ring descriptor count. **Reference: CVE-2016-8910**	NA	A-QEM-QEMU--181116/112
Denial of Service	04/11/2016	1.9	The intel_hda_xfer function in hw/audio/intel-hda.c in QEMU (aka	NA	A-QEM-QEMU--181116/113

			Quick Emulator) allows local guest OS administrators to cause a denial of service (infinite loop and CPU consumption) via an entry with the same value for buffer length and pointer position. **Reference: CVE-2016-8909**		
Denial of Service	04/11/2016	1.9	The serial_update_parameters function in hw/char/serial.c in QEMU (aka Quick Emulator) allows local guest OS administrators to cause a denial of service (divide-by-zero error and QEMU process crash) via vectors involving a value of divider greater than baud base. **Reference: CVE-2016-8669**	http://git.qemu.org/?p=qemu.git;a=commit;h=3592fe0c919cf27a81d8e9f9b4f269553418bb01	A-QEM-QEMU--181116/114
Denial of Service	04/11/2016	1.9	The rocker_io_writel function in hw/net/rocker/rocker.c in QEMU (aka Quick Emulator) allows local guest OS administrators to cause a denial of service (out-of-bounds read and QEMU process crash) by leveraging failure to limit DMA buffer	NA	A-QEM-QEMU--181116/115

			size. **Reference: CVE-2016-8668**		
Denial of Service	04/11/2016	1.9	The rc4030_write function in hw/dma/rc4030.c in QEMU (aka Quick Emulator) allows local guest OS administrators to cause a denial of service (divide-by-zero error and QEMU process crash) via a large interval timer reload value. **Reference: CVE-2016-8667**	NA	A-QEM-QEMU--181116/116
Denial of Service	04/11/2016	1.9	The v9fs_iov_vunmarshal function in fsdev/9p-iov-marshal.c in QEMU (aka Quick Emulator) allows local guest OS administrators to cause a denial of service (NULL pointer dereference and QEMU process crash) by sending an empty string parameter to a 9P operation. **Reference: CVE-2016-8578**	NA	A-QEM-QEMU--181116/117
Denial of Service	04/11/2016	1.9	Memory leak in the v9fs_read function in hw/9pfs/9p.c in QEMU (aka Quick Emulator) allows local guest OS	http://git.qemu.org/?p=qemu.git;a=commit;h=e95c9a493a5a8d6f969e86c9f19f80ffe6587e19	A-QEM-QEMU--181116/118

			administrators to cause a denial of service (memory consumption) via vectors related to an I/O read operation. **Reference: CVE-2016-8577**		
Denial of Service	04/11/2016	1.9	The xhci_ring_fetch function in hw/usb/hcd-xhci.c in QEMU (aka Quick Emulator) allows local guest OS administrators to cause a denial of service (infinite loop and QEMU process crash) by leveraging failure to limit the number of link Transfer Request Blocks (TRB) to process. **Reference: CVE-2016-8576**	http://git.qemu.org/?p=qemu.git;a=commit;h=05f43d44e4bc26611ce25fd7d726e483f73363ce	A-QEM-QEMU--181116/119
Sparkjava					
Spark Spark is a micro web framework that lets you focus on writing your code, not boilerplate code.					
Directory Traversal	04/11/2016	5	Directory traversal vulnerability in Spark 2.5 allows remote attackers to read arbitrary files via a .. (dot dot) in the URI. **Reference: CVE-2016-9177**	https://github.com/perwendel/spark/issues/700	A-SPA-SPARK--181116/120
Sybase					
Adaptive Server Enterprise SAP ASE (Adaptive Server Enterprise), originally known as Sybase SQL Server, and also commonly known as Sybase DB or ASE, is a relational model database server product for businesses developed by Sybase Corporation which became part of SAP AG.					
SQL Injection	03/11/2016	7.5	SAP ASE 16.0 SP02	https://www.tru	A-SYB-

			PL03 and prior versions allow attackers who own SourceDB and TargetDB databases to elevate privileges to sa (system administrator) via dbcc import_sproc SQL injection. **Reference: CVE-2016-7402**	stwave.com/Resources/Security-Advisories/Advisories/TWSL2016-017/?fid=8409	ADAPT--181116/121
Teradata					
Studio Express Teradata Studio Express provides an information discovery tool that retrieves data from Aster, Teradata, and Hadoop Database systems and allows the data to be manipulated and stored on the desktop. It is built on the Eclipse Rich Client Platform (RCP).					
NA	10/11/2016	7.2	The installation script studioexpressinstall for Teradata Studio Express 15.12.00.00 creates files in /tmp insecurely. A malicious local user could create a symlink in /tmp and possibly clobber system files or perhaps elevate privileges. **Reference: CVE-2016-7490**	http://www.vapidlabs.com/advisory.php?v=174	A-TER-STUDI--181116/122
Virtual Machine A virtual machine is a software computer that, like a physical computer, runs an operating system and applications. The virtual machine is comprised of a set of specification and configuration files and is backed by the physical resources of a host.					
Execute Code	10/11/2016	10	Teradata Virtual Machine Community Edition v15.10's perl script /opt/teradata/gsctools/bin/t2a.pl	http://www.vapidlabs.com/advisory.php?v=173	A-TER-VIRTU--181116/123

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

			creates files in /tmp in an insecure manner, this may lead to elevated code execution. **Reference: CVE-2016-7489**		
Execute Code	10/11/2016	7.2	Teradata Virtual Machine Community Edition v15.10 has insecure file permissions on /etc/luminex/pkg mgr. These could allow a local user to modify its contents and execute commands as root. **Reference: CVE-2016-7488**	http://www.vapidlabs.com/advisory.php?v=172	A-TER-VIRTU--181116/124
Operating System (OS)					
Canonical; Debian; Linux; Redhat					
Ubuntu Core; Ubuntu Linux/Debian Linux/Linux Kernel/Enterprise Linux; Enterprise Linux Aus; Enterprise Linux Eus; Enterprise Linux Long Life; Enterprise Linux Tus Ubuntu is a Debian based Linux Operating System; Enterprise Linux is any distribution of the open source Linux operating system for use on corporate or small business servers, desktops, workstations and mobile deployments.					
Gain Privileges	10/11/2016	7.2	Race condition in mm/gup.c in the Linux kernel 2.x through 4.x before 4.8.3 allows local users to gain privileges by leveraging incorrect handling of a copy-on-write (COW) feature to write to a read-only memory mapping, as exploited in the wild in October 2016, aka "Dirty COW."	https://github.com/torvalds/linux/commit/19be0eaffa3ac7d8eb6784ad9bdbc7d67ed8e619	O-CAN-UBUNT--181116/125

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-2016-5195		
Cisco					
Asr 5000 Software: NA					
Denial of Service	03/11/2016	5	A vulnerability in the Slowpath of StarOS for Cisco ASR 5500 Series routers with Data Processing Card 2 (DPC2) could allow an unauthenticated, remote attacker to cause a subset of the subscriber sessions to be disconnected, resulting in a partial denial of service (DoS) condition. This vulnerability affects Cisco ASR 5500 devices with Data Processing Card 2 (DPC2) running StarOS 18.0 or later. More Information: CSCvb12081. Known Affected Releases: 18.7.4 19.5.0 20.0.2.64048 20.2.3 21.0.0. Known Fixed Releases: 18.7.4 18.7.4.65030 18.8.M0.65044 19.5.0 19.5.0.65092 19.5.M0.65023 19.5.M0.65050 20.2.3 20.2.3.64982 20.2.3.65017 20.2.a4.65307	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161102-asr	O-CIS-ASR 5--181116/126

			20.3.M0.64984 20.3.M0.65029 20.3.M0.65037 20.3.M0.65071 20.3.T0.64985 20.3.T0.65031 20.3.T0.65043 20.3.T0.65067 21.0.0 21.0.0.65256 21.0.M0.64922 21.0.M0.64983 21.0.M0.65140 21.0.V0.65150 21.1.A0.64932 21.1.A0.64987 21.1.A0.65145 21.1.PP0.65270 21.1.R0.65130 21.1.R0.65135 21.1.R0.65154 21.1.VC0.65203 21.2.A0.65147. **Reference: CVE-2016-6455**		
Ios Xe IOS XE represents the continuing evolution of Cisco's pre-eminent IOS operating system which is used on most Cisco systems routers and network switches.					
Execute Code; Overflow	03/11/2016	10	Vulnerability in the Transaction Language 1 (TL1) code of Cisco ASR 900 Series routers could allow an unauthenticated, remote attacker to cause a reload of, or remotely execute code on, the affected system. This vulnerability affects Cisco ASR 900 Series Aggregation Services Routers (ASR902, ASR903, and ASR907) that	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161102-tl1	O-CIS-IOS X--181116/127

			are running the following releases of Cisco IOS XE Software: 3.17.0S 3.17.1S 3.17.2S 3.18.0S 3.18.1S. More Information: CSCuy15175. Known Affected Releases: 15.6(1)S 15.6(2)S. Known Fixed Releases: 15.6(1)S2.12 15.6(1.17)S0.41 15.6(1.17)SP 15.6(2)SP 16.4(0.183) 16.5(0.10). **Reference: CVE-2016-6441**		
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 (or simply Windows) is a metafamily of graphical operating systems developed, marketed, and sold by Microsoft. It consists of several families of operating systems, each of which cater to a certain sector of the computing industry with the OS typically associated with IBM PC compatible architecture.					
Gain Information	10/11/2016	2.1	Virtual Secure Mode in Microsoft Windows 10 allows local users to obtain sensitive information via a crafted application, aka "Virtual Secure Mode Information Disclosure Vulnerability." **Reference: CVE-2016-7220**	http://technet.microsoft.com/en-us/security/bulletin/ms16-137	O-MIC-WINDO--181116/128
Gain Privileges	10/11/2016	7.2	The kernel-mode drivers in Microsoft Windows Server 2008 R2 SP1,	http://technet.microsoft.com/en-us/security/bulletin/ms16-135	O-MIC-WINDO--181116/129

			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-2016-7246**		
Execute Code; Overflow; Memory Corruption	10/11/2016	9.3	Animation Manager in Microsoft Windows Server 2008 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 Animation Manager Memory Corruption Vulnerability." **Reference: CVE-2016-7205**	http://technet.microsoft.com/en-us/security/bulletin/ms16-132	O-MIC-WINDO--181116/130
Gain Privileges	10/11/2016	7.2	Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1,	http://technet.microsoft.com/en-us/security/bulletin/ms16-137	O-MIC-WINDO--181116/131

			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 mishandle caching for NTLM password-change requests, which allows local users to gain privileges via a crafted application, aka "Windows NTLM Elevation of Privilege Vulnerability." **Reference: CVE-2016-7238**		
Denial of Service	10/11/2016	6.8	Local Security Authority Subsystem Service (LSASS) 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 authenticated users to cause a denial of service (system hang) via a crafted request, aka "Local	http://technet.microsoft.com/en-us/security/bulletin/ms16-137	O-MIC-WINDO--181116/132

			Security Authority Subsystem Service Denial of Service Vulnerability." **Reference: CVE-2016-7237**		
Gain Privileges	10/11/2016	7.2	Input Method Editor (IME) 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 DLL loading, which allows local users to gain privileges via unspecified vectors, aka "Windows IME Elevation of Privilege Vulnerability." **Reference: CVE-2016-7221**	http://technet.microsoft.com/en-us/security/bulletin/ms16-130	O-MIC-WINDO--181116/133
Gain Information	10/11/2016	1.9	Bowser.sys 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,	http://technet.microsoft.com/en-us/security/bulletin/ms16-135	O-MIC-WINDO--181116/134

			and Windows Server 2016 allows local users to obtain sensitive information via a crafted application, aka "Windows Bowser.sys Information Disclosure Vulnerability." **Reference: CVE-2016-7218**		
Gain Privileges	10/11/2016	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-2016-7215**	http://technet.microsoft.com/en-us/security/bulletin/ms16-135	O-MIC-WINDO--181116/135
Bypass; Gain Information	10/11/2016	2.1	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,	http://technet.microsoft.com/en-us/security/bulletin/ms16-135	O-MIC-WINDO--181116/136

			Windows 10 Gold, 1511, and 1607, and Windows Server 2016 allow local users to bypass the ASLR protection mechanism via a crafted application, aka "Win32k Information Disclosure Vulnerability." **Reference: CVE-2016-7214**		
Execute Code	10/11/2016	9.3	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 remote attackers to execute arbitrary code via a crafted image file, aka "Windows Remote Code Execution Vulnerability." **Reference: CVE-2016-7212**	http://technet.microsoft.com/en-us/security/bulletin/ms16-130	O-MIC-WINDO--181116/137
Gain Information	10/11/2016	4.3	atmfd.dll in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2,	http://technet.microsoft.com/en-us/security/bulletin/ms16-132	O-MIC-WINDO--181116/138

			Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 allows remote attackers to obtain sensitive information from process memory via a crafted Open Type font on a web site, aka "Open Type Font Information Disclosure Vulnerability." **Reference: CVE-2016-7210**		
Overflow; Gain Privileges	10/11/2016	9.3	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 gain privileges via a crafted application, aka "Windows Common Log File System Driver Elevation of Privilege Vulnerability," a different vulnerability than CVE-2016-0026, CVE-2016-3332,	http://technet.microsoft.com/en-us/security/bulletin/ms16-134	O-MIC-WINDO--181116/139

			CVE-2016-3333, CVE-2016-3334, CVE-2016-3335, CVE-2016-3338, CVE-2016-3340, CVE-2016-3342, and CVE-2016-3343. **Reference: CVE-2016-7184**		
Overflow; Gain Privileges	10/11/2016	9.3	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 gain privileges via a crafted application, aka "Windows Common Log File System Driver Elevation of Privilege Vulnerability," a different vulnerability than CVE-2016-0026, CVE-2016-3332, CVE-2016-3333, CVE-2016-3334, CVE-2016-3335, CVE-2016-3338, CVE-2016-3340, CVE-2016-3342, and CVE-2016-7184.	http://technet.microsoft.com/en-us/security/bulletin/ms16-134	O-MIC-WINDO--181116/140

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-2016-3343		
Overflow; Gain Privileges	10/11/2016	9.3	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 gain privileges via a crafted application, aka "Windows Common Log File System Driver Elevation of Privilege Vulnerability," a different vulnerability than CVE-2016-0026, CVE-2016-3332, CVE-2016-3333, CVE-2016-3334, CVE-2016-3335, CVE-2016-3338, CVE-2016-3340, CVE-2016-3343, and CVE-2016-7184. **Reference: CVE-2016-3342**	http://technet.microsoft.com/en-us/security/bulletin/ms16-134	O-MIC-WINDO--181116/141
Overflow; Gain Privileges	10/11/2016	9.3	The Common Log File System (CLFS) driver in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2	http://technet.microsoft.com/en-us/security/bulletin/ms16-134	O-MIC-WINDO--181116/142

			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 gain privileges via a crafted application, aka "Windows Common Log File System Driver Elevation of Privilege Vulnerability," a different vulnerability than CVE-2016-0026, CVE-2016-3332, CVE-2016-3333, CVE-2016-3334, CVE-2016-3335, CVE-2016-3338, CVE-2016-3342, CVE-2016-3343, and CVE-2016-7184. **Reference: CVE-2016-3340**		
Overflow; Gain Privileges	10/11/2016	9.3	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	http://technet.microsoft.com/en-us/security/bulletin/ms16-134	O-MIC-WINDO--181116/143

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

			Server 2016 allows local users to gain privileges via a crafted application, aka "Windows Common Log File System Driver Elevation of Privilege Vulnerability," a different vulnerability than CVE-2016-0026, CVE-2016-3332, CVE-2016-3333, CVE-2016-3334, CVE-2016-3335, CVE-2016-3340, CVE-2016-3342, CVE-2016-3343, and CVE-2016-7184. **Reference: CVE-2016-3338**		
Overflow; Gain Privileges	10/11/2016	9.3	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 gain privileges via a crafted application, aka "Windows Common Log File System Driver Elevation of	http://technet.microsoft.com/en-us/security/bulletin/ms16-134	O-MIC-WINDO--181116/144

			Privilege Vulnerability," a different vulnerability than CVE-2016-0026, CVE-2016-3332, CVE-2016-3333, CVE-2016-3334, CVE-2016-3338, CVE-2016-3340, CVE-2016-3342, CVE-2016-3343, and CVE-2016-7184. **Reference: CVE-2016-3335**		
Overflow; Gain Privileges	10/11/2016	9.3	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 gain privileges via a crafted application, aka "Windows Common Log File System Driver Elevation of Privilege Vulnerability," a different vulnerability than CVE-2016-0026, CVE-2016-3332, CVE-2016-3333, CVE-2016-3335,	http://technet.microsoft.com/en-us/security/bulletin/ms16-134	O-MIC-WINDO--181116/145

			CVE-2016-3338, CVE-2016-3340, CVE-2016-3342, CVE-2016-3343, and CVE-2016-7184. **Reference: CVE-2016-3334**		
Overflow; Gain Privileges	10/11/2016	9.3	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 gain privileges via a crafted application, aka "Windows Common Log File System Driver Elevation of Privilege Vulnerability," a different vulnerability than CVE-2016-0026, CVE-2016-3332, CVE-2016-3334, CVE-2016-3335, CVE-2016-3338, CVE-2016-3340, CVE-2016-3342, CVE-2016-3343, and CVE-2016-7184. **Reference: CVE-2016-3333**	http://technet.microsoft.com/en-us/security/bulletin/ms16-134	O-MIC-WINDO--181116/146

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

Overflow; Gain Privileges	10/11/2016	9.3	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 gain privileges via a crafted application, aka "Windows Common Log File System Driver Elevation of Privilege Vulnerability," a different vulnerability than CVE-2016-0026, CVE-2016-3333, CVE-2016-3334, CVE-2016-3335, CVE-2016-3338, CVE-2016-3340, CVE-2016-3342, CVE-2016-3343, and CVE-2016-7184. **Reference: CVE-2016-3332**	http://technet.microsoft.com/en-us/security/bulletin/ms16-134	O-MIC-WINDO--181116/147
Overflow; Gain Privileges	10/11/2016	9.3	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,	http://technet.microsoft.com/en-us/security/bulletin/ms16-134	O-MIC-WINDO--181116/148

			Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 allows local users to gain privileges via a crafted application, aka "Windows Common Log File System Driver Elevation of Privilege Vulnerability," a different vulnerability than CVE-2016-3332, CVE-2016-3333, CVE-2016-3334, CVE-2016-3335, CVE-2016-3338, CVE-2016-3340, CVE-2016-3342, CVE-2016-3343, and CVE-2016-7184. **Reference: CVE-2016-0026**		
Execute Code	10/11/2016	9.3	Microsoft Video Control in Microsoft Windows Vista SP2, Windows 7 SP1, Windows 8.1, Windows RT 8.1, and Windows 10 Gold, 1511, and 1607 allows remote attackers to execute arbitrary code via a crafted file, aka "Microsoft Video Control Remote Code Execution	http://technet.microsoft.com/en-us/security/bulletin/ms16-131	O-MIC-WINDO--181116/149

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

			Vulnerability." **Reference: CVE-2016-7248**		
Bypass	10/11/2016	5	Microsoft Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 allow physically proximate attackers to bypass the Secure Boot protection mechanism via a crafted boot policy, aka "Secure Boot Component Vulnerability." **Reference: CVE-2016-7247**	http://technet.microsoft.com/en-us/security/bulletin/ms16-140	O-MIC-WINDO--181116/150
Gain Privileges	10/11/2016	3.6	Virtual Hard Disk Driver in Microsoft Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 does not properly restrict access to files, which allows local users to gain privileges via a crafted application, aka "VHD Driver Elevation of Privilege Vulnerability." **Reference: CVE-2016-7224**	http://technet.microsoft.com/en-us/security/bulletin/ms16-138	O-MIC-WINDO--181116/151

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

Gain Privileges	10/11/2016	3.6	Virtual Hard Disk Driver in Microsoft Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 does not properly restrict access to files, which allows local users to gain privileges via a crafted application, aka "VHD Driver Elevation of Privilege Vulnerability." **Reference: CVE-2016-7223**	http://technet.microsoft.com/en-us/security/bulletin/ms16-138	O-MIC-WINDO--181116/152
Execute Code; Overflow; Memory Corruption	10/11/2016	9.3	Media Foundation in Microsoft 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 "Media Foundation Memory Corruption Vulnerability." **Reference: CVE-2016-7217**	http://technet.microsoft.com/en-us/security/bulletin/ms16-132	O-MIC-WINDO--181116/153
Gain Privileges	10/11/2016	3.6	Virtual Hard Disk Driver in Windows 10 Gold, 1511, and 1607 and Windows	http://technet.microsoft.com/en-us/security/bulletin/ms16-138	O-MIC-WINDO--181116/154

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

			Server 2016 does not properly restrict access to files, which allows local users to gain privileges via a crafted application, aka "VHD Driver Elevation of Privilege Vulnerability." **Reference: CVE-2016-7226**		
Gain Privileges	10/11/2016	3.6	Virtual Hard Disk Driver in Windows 10 Gold, 1511, and 1607 and Windows Server 2016 does not properly restrict access to files, which allows local users to gain privileges via a crafted application, aka "VHD Driver Elevation of Privilege Vulnerability." **Reference: CVE-2016-7225**	http://technet.microsoft.com/en-us/security/bulletin/ms16-138	O-MIC-WINDO--181116/155
Gain Privileges	10/11/2016	7.2	Task Scheduler in Microsoft Windows 10 Gold, 1511, and 1607 and Windows Server 2016 allows local users to gain privileges via a crafted UNC pathname in a task, aka "Task Scheduler Elevation of Privilege Vulnerability." **Reference: CVE-2016-7222**	http://technet.microsoft.com/en-us/security/bulletin/ms16-130	O-MIC-WINDO--181116/156

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

Gain Privileges	10/11/2016	2.1	The kernel API in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 mishandles permissions, which allows local users to gain privileges via a crafted application, aka "Windows Kernel Elevation of Privilege Vulnerability." **Reference: CVE-2016-7216**	http://technet.microsoft.com/en-us/security/bulletin/ms16-139	O-MIC-WINDO--181116/157
Samsung					
Samsung Mobile Samsung is the largest mobile phone maker in its home market of South Korea, and the third largest in the world. In addition to mobile phones and related devices, the company also manufacturers things such as televisions, cameras, and electronic components.					
NA	03/11/2016	7.8	A vulnerability on Samsung Mobile L(5.0/5.1) and M(6.0) devices with the Exynos7420 chipset exists because of a NULL pointer dereference in the fimg2d driver. The patch (aka "SVE-2016-6248: SystemUI Security issue") verifies if the object is null before dereferencing it. **Reference: CVE-2016-7160**	http://security.samsungmobile.com/smrupdate.html#SMR-SEP-2016	O-SAM-SAMSU--181116/158
Denial of Service; Overflow	11/11/2016	7.8	Integer overflow in SystemUI in KK(4.4) and	http://security.samsungmobile.com/smrupdate.ht	O-SAM-SAMSU--181116/159

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

			L(5.0/5.1) on Samsung Note devices allows attackers to cause a denial of service (UI restart) via vectors involving APIs and an activity that computes an out-of-bounds array index, aka SVE-2016-6906. **Reference: CVE-2016-9277**	ml#SMR-NOV-2016	