Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Application (A)					
Admidio					
Admidio Admidio is a free online membership management, which is optimized for associations, groups and organizations.					
SQL Injection	07-03-2017	9	SQL Injection was discovered in adm_program/modules/dates/dates_function.php in Admidio 3.2.5. The POST parameter dat_cat_id is concatenated into a SQL query without any input validation/sanitization. **CVE ID: CVE-2017-6492**	https://github.com/hamkovic/Admidio-3.2.5-SQLi	A-ADM-ADMID-110417/01
SQL Injection	24-03-2017	9	SQL Injection was discovered in adm_program/modules/dates/dates_function.php in Admidio 3.2.5. The POST parameter dat_cat_id is concatenated into a SQL query without any input validation/sanitization. **CVE ID: CVE-2017-6492**	NA	A-ADM-ADMID-110417/02
Adobe					
Flash Player Adobe Flash Player is a lightweight browser plug-in and rich Internet application runtime that delivers consistent and engaging user experiences, stunning audio/video playback, and exciting gameplay.					
Execute Code	16-03-2017	10	Adobe Flash Player versions 24.0.0.221 and earlier have an exploitable use after free vulnerability related to an interaction between the privacy user interface and the ActionScript 2 Camera object. Successful exploitation could lead to arbitrary code execution. **CVE ID: CVE-2017-3003**	https://helpx.adobe.com/security/products/flash-player/apsb17-07.html	A-ADO-FLASH-110417/03
Execute Code	16-03-2017	10	Adobe Flash Player versions 24.0.0.221 and earlier have an exploitable use after free vulnerability in the	https://helpx.adobe.com/security/products/flash	A-ADO-FLASH-110417/04

			ActionScript2 TextField object related to the variable property. Successful exploitation could lead to arbitrary code execution. **CVE ID: CVE-2017-3002**	-player/apsb17-07.html	
Execute Code	16-03-2017	10	Adobe Flash Player versions 24.0.0.221 and earlier have an exploitable use after free vulnerability related to garbage collection in the ActionScript 2 VM. Successful exploitation could lead to arbitrary code execution. **CVE ID: CVE-2017-3001**	https://helpx.adobe.com/security/products/flash-player/apsb17-07.html	A-ADO-FLASH-110417/04
Gain Information	16-03-2017	5	Adobe Flash Player versions 24.0.0.221 and earlier have a vulnerability in the random number generator used for constant blinding. Successful exploitation could lead to information disclosure. **CVE ID: CVE-2017-3000**	https://helpx.adobe.com/security/products/flash-player/apsb17-07.html	A-ADO-FLASH-110417/05
Execute Code Overflow Mem. Corr.	16-03-2017	10	Adobe Flash Player versions 24.0.0.221 and earlier have an exploitable memory corruption vulnerability in the Primetime TVSDK functionality related to hosting playback surface. Successful exploitation could lead to arbitrary code execution. **CVE ID: CVE-2017-2999**	https://helpx.adobe.com/security/products/flash-player/apsb17-07.html	A-ADO-FLASH-110417/06
Execute Code Overflow Mem. Corr.	15-03-2017	10	Adobe Flash Player versions 24.0.0.221 and earlier have an exploitable memory corruption vulnerability in the Primetime TVSDK API functionality related to timeline interactions. Successful exploitation could lead to arbitrary code execution. **CVE ID: CVE-2017-2998**	https://helpx.adobe.com/security/products/flash-player/apsb17-07.html	A-ADO-FLASH-110417/07
Execute Code Overflow	15-03-2017	10	Adobe Flash Player versions 24.0.0.221 and earlier have an exploitable buffer overflow / underflow vulnerability in the Primetime TVSDK that supports	https://helpx.adobe.com/security/products/flash-	A-ADO-FLASH-110417/08

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

			customizing ad information. Successful exploitation could lead to arbitrary code execution. **CVE ID: CVE-2017-2997**	player/apsb 17-07.html	
Execute Code	16-03-2017	10	Adobe Flash Player versions 24.0.0.221 and earlier have an exploitable use after free vulnerability related to an interaction between the privacy user interface and the ActionScript 2 Camera object. Successful exploitation could lead to arbitrary code execution. **CVE ID: CVE-2017-3003**	https://helpx.adobe.com/security/products/flash-player/apsb17-07.html	A-ADO-FLASH-110417/09
Execute Code	16-03-2017	10	Adobe Flash Player versions 24.0.0.221 and earlier have an exploitable use after free vulnerability in the ActionScript2 TextField object related to the variable property. Successful exploitation could lead to arbitrary code execution. **CVE ID: CVE-2017-3002**	https://helpx.adobe.com/security/products/flash-player/apsb17-07.html	A-ADO-FLASH-110417/10
Execute Code	16-03-2017	10	Adobe Flash Player versions 24.0.0.221 and earlier have an exploitable use after free vulnerability related to garbage collection in the ActionScript 2 VM. Successful exploitation could lead to arbitrary code execution. **CVE ID: CVE-2017-3001**	https://helpx.adobe.com/security/products/flash-player/apsb17-07.html	A-ADO-FLASH-110417/11
Gain Information	16-03-2017	5	Adobe Flash Player versions 24.0.0.221 and earlier have a vulnerability in the random number generator used for constant blinding. Successful exploitation could lead to information disclosure. **CVE ID: CVE-2017-3000**	https://helpx.adobe.com/security/products/flash-player/apsb17-07.html	A-ADO-FLASH-110417/12
Execute Code Overflow Mem. Corr.	16-03-2017	10	Adobe Flash Player versions 24.0.0.221 and earlier have an exploitable memory corruption vulnerability in the Primetime TVSDK functionality related to	https://helpx.adobe.com/security/products/flash-	A-ADO-FLASH-110417/13

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

			hosting playback surface. Successful exploitation could lead to arbitrary code execution. **CVE ID: CVE-2017-2999**	player/apsb17-07.html	
Shockwave Player Shockwave Player is the web standard for powerful multimedia playback. Shockwave Player allows you to view interactive web content like games, business presentations, entertainment, and advertisements from your web browser.					
NA	15-03-2017	6.8	Adobe Shockwave versions 12.2.7.197 and earlier have an insecure library loading (DLL hijacking) vulnerability. Successful exploitation could lead to escalation of privilege. **CVE ID: CVE-2017-2983**	https://helpx.adobe.com/security/products/shockwave/apsb17-08.html	A-ADO-SHOCK-110417/14
Agora-project					
Agora-project A temporary European newsroom for journalists collaborating on the biggest challenges facing Europe.					
Cross Site Scripting	09-03-2017	4.3	XSS in Agora-Project 3.2.2 exists with an index.php?ctrl=file&targetObjId=fileFolder-2&targetObjIdChild=[XSS] attack. **CVE ID: CVE-2017-6562**	https://packetstormsecurity.com/files/141507/Agora-Project-3.2.2-Cross-Site-Scripting.html	A-AGO-AGORA-110417/15
Cross Site Scripting	09-03-2017	4.3	XSS in Agora-Project 3.2.2 exists with an index.php?ctrl=object&action=[XSS] attack. **CVE ID: CVE-2017-6561**	https://packetstormsecurity.com/files/141507/Agora-Project-3.2.2-Cross-Site-Scripting.html	A-AGO-AGORA-110417/15
Cross Site Scripting	09-03-2017	4.3	XSS in Agora-Project 3.2.2 exists with an index.php?ctrl=misc&action=[XSS]&editObjId=[XSS] attack. **CVE ID: CVE-2017-6560**	https://packetstormsecurity.com/files/141507/Agora-Project-3.2.2-Cross-Site-Scripting.html	A-AGO-AGORA-110417/16
Cross Site Scripting	09-03-2017	4.3	XSS in Agora-Project 3.2.2 exists with an index.php?disconnect=1&msgNotif[]=[XSS] attack. **CVE ID: CVE-2017-6559**	https://packetstormsecurity.com/files/141507/Agora-Project-3.2.2-Cross-Site-Scripting.html	A-AGO-AGORA-110417/17

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

Cross Site Scripting	17-03-2017	4.3	XSS in Agora-Project 3.2.2 exists with an index.php?ctrl=file&targetObjId=fileFolder-2&targetObjIdChild=[XSS] attack. **CVE ID: CVE-2017-6562**	NA	A-AGO-AGORA-110417/18
Cross Site Scripting	17-03-2017	4.3	XSS in Agora-Project 3.2.2 exists with an index.php?ctrl=object&action=[XSS] attack. **CVE ID: CVE-2017-6561**	NA	A-AGO-AGORA-110417/19
Cross Site Scripting	17-03-2017	4.3	XSS in Agora-Project 3.2.2 exists with an index.php?ctrl=misc&action=[XSS]&editObjId=[XSS] attack. **CVE ID: CVE-2017-6560**	NA	A-AGO-AGORA-110417/20
Cross Site Scripting	17-03-2017	4.3	XSS in Agora-Project 3.2.2 exists with an index.php?disconnect=1&msgNotif[]=[XSS] attack. **CVE ID: CVE-2017-6559**	NA	A-AGO-AGORA-110417/21
Alienvault					
Ossim; Unified Security Management OSSIM, AlienVault's Open Source Security Information and Event Management (SIEM) product, provides event collection, normalization and correlation; AlienVault Unified Security Management (USM) is an all-in-one platform enabling organizations of all sizes to detect and mitigate today's advanced threats.					
Execute Code; Bypass; Gain Information	17-03-2017	7.5	The logcheck function in session.inc in AlienVault OSSIM before 5.3.1, when an action has been created, and USM before 5.3.1 allows remote attackers to bypass authentication and consequently obtain sensitive information, modify the application, or execute arbitrary code as root via an "AV Report Scheduler" HTTP User-Agent header. **CVE ID: CVE-2016-7955**	https://www.alienvault.com/forums/discussion/7765/alienvault-v5-3-1-hotfix	A-ALI-OSSIM-110417/22
Alienvault;Nfsen					
Ossim;Unified Security Management/Nfsen OSSIM, AlienVault's Open Source Security Information and Event Management (SIEM) product,					

provides event collection, normalization and correlation; AlienVault Unified Security Management (USM) is an all-in-one platform enabling organizations of all sizes to detect and mitigate today's advanced threats.					
NA	28-03-2017	10	Unspecified vulnerability in AlienVault USM and OSSIM before 5.3.7 and NfSen before 1.3.8 has unknown impact and attack vectors, aka AlienVault ID ENG-104945. This is different from CVE-2017-6970 and CVE-2017-6971, and less directly relevant. (Additional details are expected to be released in a new public reference.) **CVE ID: CVE-2017-6972**	https://www.alienvault.com/forums/discussion/8698	A-ALI-OSSIM-110417/23
Execute Code	28-03-2017	9	AlienVault USM and OSSIM before 5.3.7 and NfSen before 1.3.8 allow remote authenticated users to execute arbitrary commands in a privileged context, or launch a reverse shell, via vectors involving the PHP session ID and the NfSen PHP code, aka AlienVault ID ENG-104862. **CVE ID: CVE-2017-6971**	https://www.alienvault.com/forums/discussion/8698	A-ALI-OSSIM-110417/24
Execute Code	28-03-2017	4.6	AlienVault USM and OSSIM before 5.3.7 and NfSen before 1.3.8 allow local users to execute arbitrary commands in a privileged context via an NfSen socket, aka AlienVault ID ENG-104863. **CVE ID: CVE-2017-6970**	https://www.alienvault.com/forums/discussion/8698	A-ALI-OSSIM-110417/25
Amazon					
Kindle For Pc Kindle for PC is a free application that lets you read Kindle books on your PC.					
Execute Code	24-03-2017	4.4	Untrusted search path vulnerability in Amazon Kindle for PC before 1.19 allows local users to execute arbitrary code and conduct DLL hijacking attacks via a Trojan horse DLL in the current working directory of the Kindle Setup installer.	NA	A-AMA-KINDL-110417/26

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

			CVE ID: CVE-2017-6189		
Apache					
Camel Apache Camel is a rule-based routing and mediation engine that provides a Java object-based implementation of the Enterprise Integration Patterns using an application programming interface (or declarative Java domain-specific language) to configure routing and mediation rules.					
NA	07-03-2017	7.5	Apache Camel's camel-snakeyaml component is vulnerable to Java object de-serialization vulnerability. De-serializing untrusted data can lead to security flaws. **CVE ID: CVE-2017-3159**	http://camel.apache.org/security-advisories.data/CVE ID: CVE-2017-3159.txt.asc?version=1&modificationDate=1486565167000&api=v2	A-APA-CAMEL-110417/27
NA	08-03-2017	7.5	Apache Camel's camel-jackson and camel-jacksonxml components are vulnerable to Java object de-serialization vulnerability. Camel allows to specify such a type through the 'CamelJacksonUnmarshalType' property. De-serializing untrusted data can lead to security flaws as demonstrated in various similar reports about Java de-serialization issues. **CVE ID: CVE-2016-9571**	http://camel.apache.org/security-advisories.data/CVE ID: CVE-2016-8749.txt.asc?version=2&modificationDate=1486565034000&api=v2	A-APA-CAMEL-110417/28
Struts Apache Struts is a free, open-source, MVC framework for creating elegant, modern Java web applications. It favors convention over configuration, is extensible using a plugin architecture, and ships with plugins to support REST, AJAX and JSON.					
Execute Code	15-03-2017	10	The Jakarta Multipart parser in Apache Struts 2 2.3.x before 2.3.32 and 2.5.x before 2.5.10.1 mishandles file upload, which allows remote attackers to execute arbitrary commands via a #cmd= string in a crafted Content-Type HTTP header, as exploited in the wild in March 2017.	https://cwiki.apache.org/confluence/display/WW/S2-045	A-APA-STRUT-110417/29

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

			CVE ID: CVE-2017-5638		
Tomcat The Apache Tomcat software is an open source implementation of the Java Servlet, JavaServer Pages, Java Expression Language and Java WebSocket technologies.					
Gain Information	14-03-2017	5	An information disclosure issue was discovered in Apache Tomcat 8.5.7 to 8.5.9 and 9.0.0.M11 to 9.0.0.M15 in reverse-proxy configurations. Http11InputBuffer.java allows remote attackers to read data that was intended to be associated with a different request. **CVE ID: CVE-2016-8747**	http://tomcat.apache.org/security-9.html	A-APA-TOMCA-110417/30
Gain Information	16-03-2017	5	An information disclosure issue was discovered in Apache Tomcat 8.5.7 to 8.5.9 and 9.0.0.M11 to 9.0.0.M15 in reverse-proxy configurations. Http11InputBuffer.java allows remote attackers to read data that was intended to be associated with a different request. **CVE ID: CVE-2016-8747**	http://tomcat.apache.org/security-8.html	A-APA-TOMCA-110417/31
Cross Site Scripting; Gain Information	24-03-2017	6.8	The code in Apache Tomcat 9.0.0.M1 to 9.0.0.M11, 8.5.0 to 8.5.6, 8.0.0.RC1 to 8.0.38, 7.0.0 to 7.0.72, and 6.0.0 to 6.0.47 that parsed the HTTP request line permitted invalid characters. This could be exploited, in conjunction with a proxy that also permitted the invalid characters but with a different interpretation, to inject data into the HTTP response. By manipulating the HTTP response the attacker could poison a web-cache, perform an XSS attack and/or obtain sensitive information from requests other then their own. **CVE ID: CVE-2016-6816**	https://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.0.M13	A-APA-TOMCA-110417/32

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

Microsoft					
Office;Word Microsoft Office is an office suite of applications, servers, and services developed by Microsoft.					
Denial of Service	20-03-2017	4.3	Microsoft Office 2010 SP2, Word 2010 SP2, Word 2013 RT SP1, and Word 2016 allow remote attackers to cause a denial of service (application hang) via a crafted Office document, aka "Microsoft Office Denial of Service Vulnerability." **CVE ID: CVE-2017-0029**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ CVE-2017-0029	A-MIC-OFFIC-110417/33
Server Message Block The Server Message Block (SMB) protocol is a network file sharing protocol that allows applications on a computer to read and write to files and to request services from server programs in a computer network. The SMB protocol can be used on top of its TCP/IP protocol or other network protocols.					
Execute Code	17-03-2017	9.3	The SMBv1 server 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; and Windows 10 Gold, 1511, and 1607; and Windows Server 2016 allows remote attackers to execute arbitrary code via crafted packets, aka "Windows SMB Remote Code Execution Vulnerability." This vulnerability is different from those described in CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, and CVE-2017-0146. **CVE ID: CVE-2017-0148**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ CVE-2017-0148	A-MIC-SERVE-110417/34
Execute Code	17-03-2017	9.3	The SMBv1 server 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; and Windows 10 Gold, 1511, and 1607; and Windows Server 2016 allows remote attackers to execute arbitrary code via	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ CVE-2017-0146	A-MIC-SERVE-110417/35

			crafted packets, aka "Windows SMB Remote Code Execution Vulnerability." This vulnerability is different from those described in CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, and CVE-2017-0148. **CVE ID: CVE-2017-0146**		
Execute Code	17-03-2017	9.3	The SMBv1 server 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; and Windows 10 Gold, 1511, and 1607; and Windows Server 2016 allows remote attackers to execute arbitrary code via crafted packets, aka "Windows SMB Remote Code Execution Vulnerability." This vulnerability is different from those described in CVE-2017-0143, CVE-2017-0144, CVE-2017-0146, and CVE-2017-0148. **CVE ID: CVE-2017-0145**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0145	A-MIC-SERVE-110417/36
Execute Code	17-03-2017	9.3	The SMBv1 server 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; and Windows 10 Gold, 1511, and 1607; and Windows Server 2016 allows remote attackers to execute arbitrary code via crafted packets, aka "Windows SMB Remote Code Execution Vulnerability." This vulnerability is different from those described in CVE-2017-0143, CVE-2017-0145, CVE-2017-0146, and CVE-2017-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ CVE-2017-0144	A-MIC-SERVE-110417/37

			0148. **CVE ID: CVE-2017-0144**		
Execute Code	17-03-2017	9.3	The SMBv1 server 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; and Windows 10 Gold, 1511, and 1607; and Windows Server 2016 allows remote attackers to execute arbitrary code via crafted packets, aka "Windows SMB Remote Code Execution Vulnerability." This vulnerability is different from those described in CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, and CVE-2017-0148. **CVE ID: CVE-2017-0143**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ CVE-2017-0143	A-MIC-SERVE-110417/38
Gain Information	20-03-2017	4.3	The SMBv1 server 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; and Windows 10 Gold, 1511, and 1607; and Windows Server 2016 allows remote attackers to obtain sensitive information from process memory via a crafted packets, aka "Windows SMB Information Disclosure Vulnerability." **CVE ID: CVE-2017-0147**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ CVE-2017-0147	A-MIC-SERVE-110417/39
Sharepoint Foundation SharePoint is a web-based application that integrates with Microsoft Office.					
Cross Site Scripting	20-03-2017	4.3	Microsoft SharePoint Server fails to sanitize crafted web requests, allowing remote attackers to run cross-script in local security context, aka "Microsoft SharePoint XSS Vulnerability."	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ CVE-	A-MIC-SHARE-110417/40

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

			CVE ID: CVE-2017-0107	2017-0107	
Telaxus					
Epesi EPESI CRM is an open source application dedicated for any company. It is a tool with multiple features that allows organizing, processing and storing information in every business.					
Execute Code; Cross Site Scripting	07-03-2017	4.3	Multiple Cross-Site Scripting (XSS) issues were discovered in EPESI 1.8.1.1. The vulnerabilities exist due to insufficient filtration of user-supplied data (tooltip_id, callback, args, cid) passed to the EPESI-master/modules/Utils/Tooltip/req.php URL. An attacker could execute arbitrary HTML and script code in a browser in the context of the vulnerable website. **CVE ID: CVE-2017-6491**	https://github.com/Telaxus/EPESI/issues/168	A-TEL-EPESI-110417/41
Execute Code; Cross Site Scripting	07-03-2017	4.3	Multiple Cross-Site Scripting (XSS) issues were discovered in EPESI 1.8.1.1. The vulnerabilities exist due to insufficient filtration of user-supplied data (cid, value, element, mode, tab, form_name, id) passed to the EPESI-master/modules/Utils/RecordBrowser/grid.php URL. An attacker could execute arbitrary HTML and script code in a browser in the context of the vulnerable website. **CVE ID: CVE-2017-6490**	https://github.com/Telaxus/EPESI/issues/167	A-TEL-EPESI-110417/42
Execute Code; Cross Site Scripting	07-03-2017	4.3	Multiple Cross-Site Scripting (XSS) issues were discovered in EPESI 1.8.1.1. The vulnerabilities exist due to insufficient filtration of user-supplied data (element, state, cat, id, cid) passed to the EPESI-master/modules/Utils/Watchdog/subscribe.php URL. An attacker could execute arbitrary	https://github.com/Telaxus/EPESI/issues/169	A-TEL-EPESI-110417/43

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

			HTML and script code in a browser in the context of the vulnerable website. **CVE ID: CVE-2017-6489**		
Execute Code; Cross Site Scripting	07-03-2017	4.3	Multiple Cross-Site Scripting (XSS) issues were discovered in EPESI 1.8.1.1. The vulnerabilities exist due to insufficient filtration of user-supplied data (visible, tab, cid) passed to the EPESI-master/modules/Utils/RecordBrowser/Filters/save_filters.php URL. An attacker could execute arbitrary HTML and script code in a browser in the context of the vulnerable website. **CVE ID: CVE-2017-6488**	https://github.com/Telaxus/EPESI/issues/166	A-TEL-EPESI-110417/44
Execute Code; Cross Site Scripting	07-03-2017	4.3	Multiple Cross-Site Scripting (XSS) issues were discovered in EPESI 1.8.1.1. The vulnerabilities exist due to insufficient filtration of user-supplied data (state, element, id, tab, cid) passed to the "EPESI-master/modules/Utils/RecordBrowser/favorites.php" URL. An attacker could execute arbitrary HTML and script code in a browser in the context of the vulnerable website. **CVE ID: CVE-2017-6487**	https://github.com/Telaxus/EPESI/issues/165	A-TEL-EPESI-110417/45
Execute Code; Cross Site Scripting	20-03-2017	4.3	Multiple Cross-Site Scripting (XSS) issues were discovered in EPESI 1.8.1.1. The vulnerabilities exist due to insufficient filtration of user-supplied data (tooltip_id, callback, args, cid) passed to the EPESI-master/modules/Utils/Tooltip/req.php URL. An attacker could execute arbitrary HTML and	https://github.com/Telaxus/EPESI/issues/168	A-TEL-EPESI-110417/46

			script code in a browser in the context of the vulnerable website. **CVE ID: CVE-2017-6491**		
Execute Code; Cross Site Scripting	20-03-2017	4.3	Multiple Cross-Site Scripting (XSS) issues were discovered in EPESI 1.8.1.1. The vulnerabilities exist due to insufficient filtration of user-supplied data (cid, value, element, mode, tab, form_name, id) passed to the EPESI-master/modules/Utils/RecordBrowser/grid.php URL. An attacker could execute arbitrary HTML and script code in a browser in the context of the vulnerable website. **CVE ID: CVE-2017-6490**	https://github.com/Telaxus/EPESI/issues/167	A-TEL-EPESI-110417/47
Execute Code; Cross Site Scripting	20-03-2017	4.3	Multiple Cross-Site Scripting (XSS) issues were discovered in EPESI 1.8.1.1. The vulnerabilities exist due to insufficient filtration of user-supplied data (element, state, cat, id, cid) passed to the EPESI-master/modules/Utils/Watchdog/subscribe.php URL. An attacker could execute arbitrary HTML and script code in a browser in the context of the vulnerable website. **CVE ID: CVE-2017-6489**	https://github.com/Telaxus/EPESI/issues/169	A-TEL-EPESI-110417/48
Execute Code; Cross Site Scripting	20-03-2017	4.3	Multiple Cross-Site Scripting (XSS) issues were discovered in EPESI 1.8.1.1. The vulnerabilities exist due to insufficient filtration of user-supplied data (visible, tab, cid) passed to the EPESI-master/modules/Utils/RecordBrowser/Filters/save_filters.php URL. An attacker could execute arbitrary HTML and script code in a browser in the	https://github.com/Telaxus/EPESI/issues/166	A-TEL-EPESI-110417/49

			context of the vulnerable website. **CVE ID: CVE-2017-6488**		
Telegram					
Messenger Telegram is a free cloud-based instant messaging service.					
Gain Information	15-03-2017	5	An issue was discovered in Telegram Messenger 2.6 for iOS and 1.8.2 for Android. Secret chat messages are available in cleartext in process memory and a .db file. **CVE ID: CVE-2014-8688**	https://blog.zimperium.com/telegram-hack/	A-TEL-MESSE-110417/50
Teleogistic					
Invite Anyone Plugin NA					
NA	21-03-2017	5	An issue was discovered in by-email/by-email.php in the Invite Anyone plugin before 1.3.15 for WordPress. A user is able to change the subject and the body of the invitation mail that should be immutable, which facilitates a social engineering attack. **CVE ID: CVE-2017-6955**	https://wordpress.org/plugins/invite-anyone/changelog/	A-TEL-INVIT-110417/51
Tenable					
Appliance; Nessus Tenable virtual appliances deliver power, deployment speed and all around ease of use by virtually eliminating installation, configuration and maintenance problems. Virtual appliances are virtual machines that come preconfigured with a hardened Linux operating system and an easy to manage web interface that is ready to configure					
Gain Privileges	13-03-2017	6	Tenable Nessus before 6.10.2 (as used alone or in Tenable Appliance before 4.5.0) was found to contain a flaw that allowed a remote, authenticated attacker to upload a crafted file that could be written to anywhere on the system. This could be used to subsequently gain elevated privileges on the system (e.g., after a reboot). This issue only affects installations on	http://www.tenable.com/security/tns-2017-06	A-TEN-APPLI-110417/52

			Windows. **CVE ID: CVE-2017-6543**		
Trend Micro					
Endpoint Sensor NA					
Execute Code	15-03-2017	9.3	Trend Micro Endpoint Sensor 1.6 before b1290 has a DLL hijacking vulnerability that allows remote attackers to execute arbitrary code, aka Trend Micro Vulnerability Identifier 2015-0208. **CVE ID: CVE-2017-6798**	https://success.trendmicro.com/solution/1116827	A-TRE-ENDPO-110417/53
Typo3					
Typo3 TYPO3 is a free and open source web content management system written in PHP.					
Gain Information	27-03-2017	5	TYPO3 7.6.15 sends an http request to an index.php?loginProvider URI in cases with an https Referer, which allows remote attackers to obtain sensitive cleartext information by sniffing the network and reading the userident and username fields. **CVE ID: CVE-2017-6370**	NA	A-TYP-TYPO3-110417/54
Uclibc-ng Project					
Uclibc-ng uClibc-ng is a small C library for developing embedded Linux systems.					
Denial of Service	27-03-2017	5	The __read_etc_hosts_r function in libc/inet/resolv.c in uClibc-ng before 1.0.12 allows remote DNS servers to cause a denial of service (infinite loop) via a crafted packet. **CVE ID: CVE-2016-2225**	http://repo.or.cz/uclibc-ng.git/commit/6932f2282ba0578d6ca2f21eead920d6b78bc93c	A-UCL-UCLIB-110417/55
Denial of Service	27-03-2017	5	The __decode_dotted function in libc/inet/resolv.c in uClibc-ng before 1.0.12 allows remote DNS servers to cause a denial of service (infinite loop) via vectors involving compressed items in a reply. **CVE ID: CVE-2016-2224**	https://security-tracker.debian.org/tracker/CVE ID: CVE-2016-2224	A-UCL-UCLIB-110417/56

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

Umbraco					
Umbraco Umbraco Cloud is a fully-featured open source content management system with the flexibility to run anything from small campaign or brochure sites right through to complex applications for Fortune 500's and some of the largest media sites in the world					
Cross Site Scripting	07-03-2017	5	Multiple cross-site scripting (XSS) vulnerabilities in Umbraco before 7.4.0 allow remote attackers to inject arbitrary web script or HTML via the name parameter to (1) the media page, (2) the developer data edit page, or (3) the form page. **CVE ID: CVE-2015-8815**	http://issues.umbraco.org/issue/U4-7461	A-UMB-UMBRA-110417/57
Bypass; Cross Site Request Forgery	07-03-2017	6.8	Umbraco before 7.4.0 allows remote attackers to bypass anti-forgery security measures and conduct cross-site request forgery (Cross Site Request Foregery) attacks as demonstrated by editing user account information in the templates.asmx.cs file. **CVE ID: CVE-2015-8814**	https://github.com/umbraco/Umbraco-CMS/commit/18c3345e47663a358a042652e697b988d6a380eb	A-UMB-UMBRA-110417/58
NA	07-03-2017	4.3	The Page_Load function in Umbraco.Web/umbraco.presentation/umbraco/dashboard/FeedProxy.aspx.cs in Umbraco before 7.4.0 allows remote attackers to conduct server-side request forgery (SSRF) attacks via the url parameter. **CVE ID: CVE-2015-8813**	https://github.com/umbraco/Umbraco-CMS/commit/924a016ffe7ae7ea6d516c07a7852f0095eddbce	A-UMB-UMBRA-110417/59
Uninett					
Mod Auth Mellon mod-auth-mellon is an Apache module which enables you to authenticate users of a web site against a SAML 2.0 enabled IdP. It can grant access to paths and provide attributes to other modules and applications.					
Cross Site Scripting	14-03-2017	4.3	mod_auth_mellon before 0.13.1 is vulnerable to a Cross-Site Session Transfer attack, where a user with access to one web site running on a	https://sympa.uninett.no/lists/uninett.no/arc/modmellon/	A-UNI-MODA-110417/60

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

			server can copy their session cookie to a different web site on the same server to get access to that site. **CVE ID: CVE-2017-6807**	2017-03/msg00008.html	
Unisys					
Clearpath Mcp The ClearPath MCP operating environment delivers exceptional value through a completely integrated and pretested software stack.					
Denial of Service	16-03-2017	5	The TCP/IP networking module in Unisys ClearPath MCP systems with TCP-IP-SW 57.1 before 57.152, 58.1 before 58.142, or 59.1 before 59.172, when running a TLS 1.2 service, allows remote attackers to cause a denial of service (network connectivity disruption) via a client hello with a signature_algorithms extension above those defined in RFC 5246, which triggers a full memory dump. **CVE ID: CVE-2017-5872**	https://public.support.unisys.com/common/public/vulnerability/NVD_Detail_Rpt.aspx?ID=42	A-UNI-CLEAR-110417/61
Denial of Service	16-03-2017	5	The TCP/IP networking module in Unisys ClearPath MCP systems with TCP-IP-SW 57.1 before 57.152, 58.1 before 58.142, or 59.1 before 59.172, when running a TLS 1.2 service, allows remote attackers to cause a denial of service (network connectivity disruption) via a client hello with a signature_algorithms extension above those defined in RFC 5246, which triggers a full memory dump. **CVE ID: CVE-2017-5872**	https://public.support.unisys.com/common/public/vulnerability/NVD_Detail_Rpt.aspx?ID=42	A-UNI-CLEAR-110417/62
Wp Markdown Editor Project					
Wp Markdown Editor Markdown lets you compose posts and comments with links, lists, and other styles using regular characters and punctuation marks. Markdown is used by writers and bloggers who want a quick and easy way to style their text, without having to take their hands off the keyboard, and without learning a lot of complicated codes and shortcuts.					

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

Cross Site Scripting	11-03-2017	4.3	A Stored XSS Vulnerability exists in the WP Markdown Editor (aka wp-markdown-editor) plugin 2.0.3 for WordPress. An example attack vector is a crafted IMG element in Add New Post or Edit Post. **CVE ID: CVE-2017-6804**	http://www.daimacn.com/?id=9	A-WP -WP MA-110417/63
Wuhu Project					
Wuhu NA					
Cross Site Scripting	13-03-2017	4.3	Gargaj/wuhu through 08-03-2017 is vulnerable to a reflected XSS in wuhu-master/www_admin/users.php (id parameter). **CVE ID: CVE-2017-6544**	https://github.com/Gargaj/wuhu/issues/20	A-WUH-WUHU-110417/64
Wvware					
Libwmf libwmf is a library for reading vector images in Microsoft's native Windows Metafile Format (WMF) and for either (a) displaying them in, e.g., an X window; or (b) converting them to more standard/open file formats such as, e.g., the W3C's XML-based Scaleable Vector Graphic (SVG) format.					
Denial of Service; Overflow	27-03-2017	4.3	The wmf_malloc function in api.c in libwmf 0.2.8.4 allows remote attackers to cause a denial of service (application crash) via a crafted wmf file, which triggers a memory allocation failure. **CVE ID: CVE-2016-9011**	https://bugzilla.redhat.com/show_bug.cgi?id=1388450	A-WVW-LIBWM-110417/65
Xrdp					
Xrdp Xrdp is an open source RDP server.					
Bypass	21-03-2017	7.5	xrdp 0.9.1 calls the PAM function auth_start_session() in an incorrect location, leading to PAM session modules not being properly initialized, with a potential consequence of incorrect configurations or elevation of privileges, aka a pam_limits.so bypass. **CVE ID: CVE-2017-6967**	NA	A-XRD-XRDP-110417/66

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

Yandex					
Yandex Browser Yandex Browser is a stylish and secure, with voice search and data compression.					
NA	03-03-2017	4.3	Yandex Browser for desktop before 17.1.1.227 does not show Protect (similar to Safebrowsing in Chromium) warnings in web-sites with special content-type, which could be used by remote attacker for prevention Protect warning on own malicious web-site. **CVE ID: CVE-2016-8508**	https://yandex.com/blog/security-changelogs/fixed-in-version-17-1	A-YAN-YANDE-110417/67
Gain Information	03-03-2017	4.3	Yandex Browser for iOS before 16.10.0.2357 does not properly restrict processing of facetime:// URLs, which allows remote attackers to initiate facetime-call without user's approval and obtain video and audio data from a device via a crafted web site. **CVE ID: CVE-2016-8507**	https://yandex.com/blog/security-changelogs/fixed-in-version-16-10	A-YAN-YANDE-110417/68
Ytnef Project					
Ytnef Ytnef is a program to work with procmail to decode TNEF streams (winmail.dat attachments) like those created with Outlook. Unlike other similar programs, it can also create vCalendar/vCard entries from meeting requests, address cards, and task entries.					
Overflow	13-03-2017	5	An issue was discovered in ytnef before 1.9.2. There is a potential heap-based buffer over-read on incoming Compressed RTF Streams, related to DecompressRTF() in libytnef. **CVE ID: CVE-2017-6802**	https://github.com/Yeraze/ytnef/commit/22f8346c8d4f0020a40d9f258fdb3bfc097359cc	A-YTN-YTNEF-110417/69
NA	13-03-2017	5	An issue was discovered in ytnef before 1.9.2. There is a potential out-of-bounds access with fields of Size 0 in TNEFParse() in libytnef. **CVE ID: CVE-2017-6801**	https://github.com/Yeraze/ytnef/commit/3cb0f914d6427073f262e1b2b5fd973e3043cdf7	A-YTN-YTNEF-110417/70

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

Overflow	13-03-2017	5	An issue was discovered in ytnef before 1.9.2. An invalid memory access (heap-based buffer over-read) can occur during handling of LONG data types, related to MAPIPrint() in libytnef. **CVE ID: CVE-2017-6800**	https://github.com/Yeraze/ytnef/commit/f98f5d4adc1c4bd4033638f6167c1bb95d642f89	A-YTN-YTNEF-110417/71
Zahmit Design					
Connections Business Directory Plugin NA					
Cross Site Scripting	17-03-2017	4.3	Cross-site scripting (XSS) vulnerability in includes/admin/pages/manage.php in the Connections Business Directory plugin before 8.5.9 for WordPress allows remote attackers to inject arbitrary web script or HTML via the s variable. **CVE ID: CVE-2016-0770**	https://wordpress.org/plugins/connections/changelog/	A-ZAH-CONNE-110417/72
Zammad					
Zammad Zammad is a web based open source helpdesk/customer support system					
Cross Site Scripting	14-03-2017	4.3	An issue was discovered in Zammad before 1.0.4, 1.1.x before 1.1.3, and 1.2.x before 1.2.1. XSS can be triggered via malicious HTML in a chat message or the content of a ticket article, when using either the REST API or the WebSocket API. **CVE ID: CVE-2017-5621**	https://zammad.com/de/news/security-advisory-zaa-2017-01	A-ZAM-ZAMMA-110417/73
Cross Site Scripting	14-03-2017	4.3	An XSS issue was discovered in Zammad before 1.0.4, 1.1.x before 1.1.3, and 1.2.x before 1.2.1. Attachments are opened in a new tab instead of getting downloaded. This creates an attack vector of executing code in the domain of the application. **CVE ID: CVE-2017-5620**	https://zammad.com/de/news/security-advisory-zaa-2017-01	A-ZAM-ZAMMA-110417/74

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

NA	14-03-2017	7.5	An issue was discovered in Zammad before 1.0.4, 1.1.x before 1.1.3, and 1.2.x before 1.2.1. Attackers can login with the hashed password itself (e.g., from the DB) instead of the valid password string. **CVE ID: CVE-2017-5619**	https://zammad.com/de/news/security-advisory-zaa-2017-01	A-ZAM-ZAMMA-110417/75
Cross Site Request Forgery	17-03-2017	6.8	A Cross Site Request Forgery issue was discovered in Zammad before 1.0.4, 1.1.x before 1.1.3, and 1.2.x before 1.2.1. To exploit the vulnerability, an attacker can send cross-domain requests directly to the REST API for users with a valid session cookie. **CVE ID: CVE-2017-6081**	https://zammad.com/de/news/security-advisory-zaa-2017-01	A-ZAM-ZAMMA-110417/76
NA	17-03-2017	7.5	An issue was discovered in Zammad before 1.0.4, 1.1.x before 1.1.3, and 1.2.x before 1.2.1, caused by lack of a protection mechanism involving HTTP Access-Control headers. To exploit the vulnerability, an attacker can send cross-domain requests directly to the REST API for users with a valid session cookie and receive the result. **CVE ID: CVE-2017-6080**	https://zammad.com/de/news/security-advisory-zaa-2017-01	A-ZAM-ZAMMA-110417/77
Cross Site Scripting	17-03-2017	4.3	An issue was discovered in Zammad before 1.0.4, 1.1.x before 1.1.3, and 1.2.x before 1.2.1. XSS can be triggered via malicious HTML in a chat message or the content of a ticket article, when using either the REST API or the WebSocket API. **CVE ID: CVE-2017-5621**	https://zammad.com/de/news/security-advisory-zaa-2017-01	A-ZAM-ZAMMA-110417/78
Cross Site Scripting	17-03-2017	4.3	An XSS issue was discovered in Zammad before 1.0.4, 1.1.x before 1.1.3, and 1.2.x before	https://zammad.com/de/news/secu	A-ZAM-ZAMMA-110417/79

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

			1.2.1. Attachments are opened in a new tab instead of getting downloaded. This creates an attack vector of executing code in the domain of the application. **CVE ID: CVE-2017-5620**	rity-advisory-zaa-2017-01	
NA	17-03-2017	7.5	An issue was discovered in Zammad before 1.0.4, 1.1.x before 1.1.3, and 1.2.x before 1.2.1. Attackers can login with the hashed password itself (e.g., from the DB) instead of the valid password string. **CVE ID: CVE-2017-5619**	https://zammad.com/de/news/security-advisory-zaa-2017-01	A-ZAM-ZAMMA-110417/80
Zoneminder					
Zoneminder A full-featured, open source, state-of-the-art video surveillance software system.					
Cross Site Request Forgery	07-03-2017	6.8	Cross-site request forgery vulnerability in Zoneminder 1.30 and earlier allows remote attackers to hijack the authentication of users for requests that change passwords and possibly have unspecified other impact as demonstrated by a crafted user action request to index.php. **CVE ID: CVE-2016-10206**	NA	A-ZON-ZONEM-110417/81
NA	07-03-2017	7.5	Session fixation vulnerability in Zoneminder 1.30 and earlier allows remote attackers to hijack web sessions via the ZMSESSID cookie. **CVE ID: CVE-2016-10205**	NA	A-ZON-ZONEM-110417/82
Execute Code SQL Injection	07-03-2017	7.5	SQL INJECTION injection vulnerability in Zoneminder 1.30 and earlier allows remote attackers to execute arbitrary SQL INJECTION commands via the limit parameter in a log query request to index.php. **CVE ID: CVE-2016-10204**	NA	A-ZON-ZONEM-110417/83
XSS	07-03-2017	4.3	Cross-site scripting (XSS) vulnerability in Zoneminder	NA	A-ZON-ZONEM-

			1.30 and earlier allows remote attackers to inject arbitrary web script or HTML via the name when creating a new monitor. **CVE ID: CVE-2016-10203**		110417/84
XSS	07-03-2017	4.3	Cross-site scripting (XSS) vulnerability in Zoneminder 1.30 and earlier allows remote attackers to inject arbitrary web script or HTML via the path info to index.php. **CVE ID: CVE-2016-10202**	NA	A-ZON-ZONEM-110417/85
XSS	07-03-2017	4.3	Cross-site scripting (XSS) vulnerability in Zoneminder 1.30 and earlier allows remote attackers to inject arbitrary web script or HTML via the format parameter in a download log request to index.php. **CVE ID: CVE-2016-10201**	NA	A-ZON-ZONEM-110417/86
Execute Code XSS	23-03-2017	4.3	A Cross-Site Scripting (XSS) was discovered in ZoneMinder 1.30.2. The vulnerability exists due to insufficient filtration of user-supplied data (postLoginQuery) passed to the "ZoneMinder-master/web/skins/classic/views/js/postlogin.js.php" URL. An attacker could execute arbitrary HTML and script code in a browser in the context of the vulnerable website. **CVE ID: CVE-2017-7203**	https://github.com/ZoneMinder/ZoneMinder/issues/1797	A-ZON-ZONEM-110417/87
Zziplib Project					
Zziplib The zziplib library offers the ability to easily extract data from files archived in a single zip file.					
Denial of Service	06-03-2017	4.3	seeko.c in zziplib 0.13.62 allows remote attackers to cause a denial of service (assertion failure and crash) via a crafted ZIP file.	NA	A-ZZI-ZZIPL-110417/88

			CVE ID: CVE-2017-5981		
Denial of Service	06-03-2017	4.3	The zzip_mem_entry_new function in memdisk.c in zziplib 0.13.62 allows remote attackers to cause a denial of service (NULL pointer dereference and crash) via a crafted ZIP file. **CVE ID: CVE-2017-5980**	NA	A-ZZI-ZZIPL-110417/89
Denial of Service	06-03-2017	4.3	The prescan_entry function in fseeko.c in zziplib 0.13.62 allows remote attackers to cause a denial of service (NULL pointer dereference and crash) via a crafted ZIP file. **CVE ID: CVE-2017-5979**	NA	A-ZZI-ZZIPL-110417/90
Denial of Service	06-03-2017	4.3	The zzip_mem_entry_new function in memdisk.c in zziplib 0.13.62 allows remote attackers to cause a denial of service (out-of-bounds read and crash) via a crafted ZIP file. **CVE ID: CVE-2017-5978**	NA	A-ZZI-ZZIPL-110417/91
Denial of Service	06-03-2017	4.3	The zzip_mem_entry_extra_block function in memdisk.c in zziplib 0.13.62 allows remote attackers to cause a denial of service (invalid memory read and crash) via a crafted ZIP file. **CVE ID: CVE-2017-5977**	NA	A-ZZI-ZZIPL-110417/92
Denial of Service Overflow	06-03-2017	4.3	Heap-based buffer overflow in the zzip_mem_entry_extra_block function in memdisk.c in zziplib 0.13.62 allows remote attackers to cause a denial of service (crash) via a crafted ZIP file. **CVE ID: CVE-2017-5976**	NA	A-ZZI-ZZIPL-110417/93
Denial of Service Overflow	06-03-2017	4.3	Heap-based buffer overflow in the __zzip_get64 function in fetch.c in zziplib 0.13.62 allows	NA	A-ZZI-ZZIPL-110417/94

			remote attackers to cause a denial of service (crash) via a crafted ZIP file. **CVE ID: CVE-2017-5975**		
Denial of Service Overflow	06-03-2017	4.3	Heap-based buffer overflow in the __zzip_get32 function in fetch.c in zziplib 0.13.62 allows remote attackers to cause a denial of service (crash) via a crafted ZIP file. **CVE ID: CVE-2017-5974**	NA	A-ZZI-ZZIPL-110417/95
Application/ Operating System (A/OS)					
Artifex/Debian					
Afpl Ghostscript/Debian Linux Ghostscript is a suite of software based on an interpreter for Adobe Systems' PostScript/ Debian is a popular and freely-available computer operating system that uses the Linux kernel and other program components obtained from the GNU project.					
Gain Information	08-03-2017	4.3	The getenv and filenameforall functions in Ghostscript 9.10 ignore the "-dSAFER" argument, which allows remote attackers to read data via a crafted postscript file. **CVE ID: CVE-2013-5653**	https://bugzilla.redhat.com/show_bug.cgi?id=1380327	A-OS-ART-AFPL - 110417/96
Artifex/Fedoraproject					
Mujs/Fedora MuJS is a lightweight Javascript interpreter designed for embedding in other software to extend them with scripting capabilities/ Fedora is a Linux based operating system.					
Denial of Service	27-03-2017	5	regexp.c in Artifex Software, Inc. MuJS allows attackers to cause a denial of service (NULL pointer dereference and crash) via vectors related to regular expression compilation. **CVE ID: CVE-2016-10132**	https://bugs.ghostscript.com/show_bug.cgi?id=697381	A-OS-ART-MUJS/-110417/97
Qemu/Suse					
Qemu/Linux Enterprise Desktop; Linux Enterprise Server; Linux Enterprise Server For Sap; Linux Enterprise Software Development Kit QEMU (short for Quick Emulator) is a free and open-source hosted hypervisor that performs hardware virtualization/ 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; Linux Enterprise Server for SAP Applications is a bundle of software and services that addresses the specific needs of SAP users. It is the only operating system that is optimized for all SAP software solutions; SUSE Linux Enterprise Software Development Kit is a comprehensive development tool kit that is					

designed to support developers, as well as independent hardware vendors (IHVs) and independent software vendors (ISVs), in creating applications on or porting them to SUSE Linux Enterprise 11 products.					
Denial of Service Overflow	16-03-2017	2.1	Integer overflow in the emulated_apdu_from_guest function in usb/dev-smartcard-reader.c in Quick Emulator (Qemu), when built with the CCID Card device emulator support, allows local users to cause a denial of service (application crash) via a large Application Protocol Data Units (APDU) unit. **CVE ID: CVE-2017-5898**	https://bugzilla.redhat.com/show_bug.cgi?id=1419699	A-OS-QEM-QEMU/-110417/98
Denial of Service Overflow	16-03-2017	2.1	Integer overflow in the emulated_apdu_from_guest function in usb/dev-smartcard-reader.c in Quick Emulator (Qemu), when built with the CCID Card device emulator support, allows local users to cause a denial of service (application crash) via a large Application Protocol Data Units (APDU) unit. **CVE ID: CVE-2017-5898**	https://bugzilla.redhat.com/show_bug.cgi?id=1419699	A-OS-QEM-QEMU/-110417/99
Operating System (OS)					
Asus					
Rt-ac53 Firmware NA					
NA	09-03-2017	9.3	Session hijack vulnerability in httpd in ASUS ASUSWRT on RT-AC53 3.0.0.4.380.6038 devices allows remote attackers to steal any active admin session by sending cgi_logout and asusrouter-Windows-IFTTT-1.0 in certain HTTP headers. **CVE ID: CVE-2017-6549**	https://bierbaumer.net/security/asuswrt/#session-stealing	O-ASU-RT-AC-110417/100
Execute Code Overflow	09-03-2017	10	Buffer overflows in networkmap in ASUS ASUSWRT on RT-AC53 3.0.0.4.380.6038 devices allow	https://bierbaumer.net/security/asuswrt/#remo	O-ASU-RT-AC-110417/101

			remote attackers to execute arbitrary code on the router via a long host or port in crafted multicast messages. **CVE ID: CVE-2017-6548**	te-code-execution	
Cross Site Scripting	09-03-2017	4.3	Cross-site scripting (XSS) vulnerability in httpd in ASUS ASUSWRT on RT-AC53 3.0.0.4.380.6038 devices allows remote attackers to inject arbitrary JavaScript by requesting filenames longer than 50 characters. **CVE ID: CVE-2017-6547**	https://bierbaumer.net/security/asuswrt/#cross-site-scripting-XSS	O-ASU-RT-AC-110417/102
NA	17-03-2017	9.3	Session hijack vulnerability in httpd in ASUS ASUSWRT on RT-AC53 3.0.0.4.380.6038 devices allows remote attackers to steal any active admin session by sending cgi_logout and asusrouter-Windows-IFTTT-1.0 in certain HTTP headers. **CVE ID: CVE-2017-6549**		O-ASU-RT-AC-110417/103
Execute Code; Overflow	17-03-2017	10	Buffer overflows in networkmap in ASUS ASUSWRT on RT-AC53 3.0.0.4.380.6038 devices allow remote attackers to execute arbitrary code on the router via a long host or port in crafted multicast messages. **CVE ID: CVE-2017-6548**	NA	O-ASU-RT-AC-110417/104
Cross Site Scripting	17-03-2017	4.3	Cross-site scripting (XSS) vulnerability in httpd in ASUS ASUSWRT on RT-AC53 3.0.0.4.380.6038 devices allows remote attackers to inject arbitrary JavaScript by requesting filenames longer than 50 characters. **CVE ID: CVE-2017-6547**	NA	O-ASU-RT-AC-110417/105
Asus;Trendnet					
Rt-ac66u Firmware/Tew-812dru Firmware NA					

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; Overflow	15-03-2017	10	Buffer overflow in Broadcom ACSD allows remote attackers to execute arbitrary code via a long string to TCP port 5916. This component is used on routers of multiple vendors including ASUS RT-AC66U and TRENDnet TEW-812DRU. **CVE ID: CVE-2013-4659**	NA	O-ASU-RT-AC-110417/106
Cambium Networks					
Cnpilot R200 Series Firmware The cnPilot R-series R200/R201 Family products support DHCP options 66, to update the configuration from a TFTP server and to update the firmware.					
NA	13-03-2017	10	On Cambium Networks cnPilot R200/201 devices before 4.3, there is a vulnerability involving the certificate of the device and its RSA keys, aka RBN-183. **CVE ID: CVE-2017-5859**	https://support.cambiumnetworks.com/file/3f88842a39f37b0d4ce5d43e5aa21bf1c4f9f1ca	O-CAM-CNPIL-110417/107
Canonical					
Ubuntu Linux Ubuntu is a community developed, Linux-based operating system that is perfect for laptops, desktops and servers. It contains all the applications you need - a Web browser, presentation, document and spreadsheet software, instant messaging and other applications.					
Execute Code	13-03-2017	6.9	An issue was discovered in network-manager-applet (aka network-manager-gnome) in Ubuntu 12.04 LTS, 14.04 LTS, 16.04 LTS, and 16.10. A local attacker could use this issue at the default Ubuntu login screen to access local files and execute arbitrary commands as the lightdm user. The exploitation requires physical access to the locked computer and the Wi-Fi must be turned on. An access point that lets you use a certificate to login is required as well, but it's easy to create one. Then, it's possible to open a nautilus window and browse	https://bugs.launchpad.net/ubuntu/+source/network-manager-applet/+bug/1668321	O-CAN-UBUNT-110417/108

			directories. One also can open some applications such as Firefox, which is useful for downloading malicious binaries. **CVE ID: CVE-2017-6590**		
Cisco					
Aironet Access Point Software Cisco Aironet Series wireless access points are easily deployed in networks for a branch offices, campuses, or large enterprises.					
Bypass	27-03-2017	10	A vulnerability in the web-based GUI of Cisco Mobility Express 1800 Series Access Points could allow an unauthenticated, remote attacker to bypass authentication. The attacker could be granted full administrator privileges. The vulnerability is due to improper implementation of authentication for accessing certain web pages using the GUI interface. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web interface of the affected system. A successful exploit could allow the attacker to bypass authentication and perform unauthorized configuration changes or issue control commands to the affected device. This vulnerability affects Cisco Mobility Express 1800 Series Access Points running a software version prior to 8.2.110.0. Cisco Bug IDs: CSCuy68219. **CVE ID: CVE-2017-3831**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170315-ap1800	O-CIS-AIRON-110417/109
Ios Xe Cisco IOS XE software provides a modular structure that significantly enhances software quality and performance by separating the data plane and control plan.					
Denial of	27-03-2017	7.8	A vulnerability in the DHCP	https://tool	O-CIS-IOS X-

Service			code for the Zero Touch Provisioning feature of Cisco ASR 920 Series Aggregation Services Routers could allow an unauthenticated, remote attacker to cause an affected device to reload. The vulnerability is due to a format string vulnerability when processing a crafted DHCP packet for Zero Touch Provisioning. An attacker could exploit this vulnerability by sending a specially crafted DHCP packet to an affected device. An exploit could allow the attacker to cause the device to reload, resulting in a denial of service (Denial of Service) condition. This vulnerability affects Cisco ASR 920 Series Aggregation Services Routers that are running an affected release of Cisco IOS XE Software (3.13 through 3.18) and are listening on the DHCP server port. By default, the devices do not listen on the DHCP server port. Cisco Bug IDs: CSCuy56385. **CVE ID: CVE-2017-3859**	s.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170322-ztp	110417/110
Execute Code	27-03-2017	9	A vulnerability in the web framework of Cisco IOS XE Software could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. The vulnerability is due to insufficient input validation of HTTP parameters supplied by the user. An attacker could exploit this vulnerability by authenticating to the device and submitting crafted input to the affected	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170322-xeci	O-CIS-IOS X-110417/111

			web page parameter. The user must be authenticated to access the affected parameter. A successful exploit could allow the attacker to execute commands with root privileges. This vulnerability affects Cisco devices running Cisco IOS XE Software Release 16.2.1, if the HTTP Server feature is enabled for the device. The newly redesigned, web-based administration interface was introduced in the Denali 16.2 Release of Cisco IOS XE Software. The web-based administration interface in earlier releases of Cisco IOS XE Software is not affected by this vulnerability. Cisco Bug IDs: CSCuy83069. **CVE ID: CVE-2017-3858**		
IOS; Ios Xe iOS (formerly iPhone OS) is a mobile operating system created and developed by Apple Inc. exclusively for its hardware; Cisco IOS XE software provides a modular structure that significantly enhances software quality and performance by separating the data plane and control plan.					
Denial of Service	27-03-2017	7.1	A vulnerability in the Autonomic Networking Infrastructure (ANI) feature of Cisco IOS Software (15.4 through 15.6) and Cisco IOS XE Software (3.7 through 3.18, and 16) could allow an unauthenticated, remote attacker to cause a denial of service (Denial of Service) condition. The vulnerability is due to incomplete input validation on certain crafted packets. An attacker could exploit this vulnerability by sending a crafted IPv6 packet to a device that is running a Cisco IOS Software or Cisco IOS XE Software release that	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170320-aniipv6	O-CIS-IOS;I-110417/112

			supports the ANI feature. A device must meet two conditions to be affected by this vulnerability: (1) the device must be running a version of Cisco IOS Software or Cisco IOS XE Software that supports ANI (regardless of whether ANI is configured); and (2) the device must have a reachable IPv6 interface. An exploit could allow the attacker to cause the affected device to reload. Cisco Bug IDs: CSCvc42729. **CVE ID: CVE-2017-3850**		
Netflow Generation Appliance Software The Cisco NetFlow Generation Appliance (NGA) 3340 introduces a highly scalable, cost-effective architecture for cross-device flow generation in today's high-performance data centers.					
Denial of Service	03-03-2017	5	A vulnerability in the Stream Control Transmission Protocol (SCTP) decoder of the Cisco NetFlow Generation Appliance (NGA) with software before 1.1(1a) could allow an unauthenticated, remote attacker to cause the device to hang or unexpectedly reload, causing a denial of service (Denial of Service) condition. The vulnerability is due to incomplete validation of SCTP packets being monitored on the NGA data ports. An attacker could exploit this vulnerability by sending malformed SCTP packets on a network that is monitored by an NGA data port. SCTP packets addressed to the IP address of the NGA itself will not trigger this vulnerability. An exploit could allow the attacker to cause the appliance to become unresponsive or	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170301-nga	O-CIS-NETFL-110417/113

			reload, causing a Denial of Service condition. User interaction could be needed to recover the device using the reboot command from the CLI. The following Cisco NetFlow Generation Appliances are vulnerable: NGA 3140, NGA 3240, NGA 3340. Cisco Bug IDs: CSCvc83320. **CVE ID: CVE-2017-3826**		
Nx-os NX-OS is a network operating system for the Nexus-series Ethernet switches and MDS-series Fibre Channel storage area network switches made by Cisco Systems.					
Denial of Service; Overflow	21-03-2017	5	A Denial of Service vulnerability in the Telnet remote login functionality of Cisco NX-OS Software running on Cisco Nexus 9000 Series Switches could allow an unauthenticated, remote attacker to cause a Telnet process used for login to terminate unexpectedly and the login attempt to fail. There is no impact to user traffic flowing through the device. Affected Products: This vulnerability affects Cisco Nexus 9000 Series Switches that are running Cisco NX-OS Software and are configured to allow remote Telnet connections to the device. More Information: CSCux46778. Known Affected Releases: 7.0(3)I3(0.170). Known Fixed Releases: 7.0(3)I3(1) 7.0(3)I3(0.257) 7.0(3)I3(0.255) 7.0(3)I2(2e) 7.0(3)F1(1.22) 7.0(3)F1(1). **CVE ID: CVE-2017-3878**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170315-nss	O-CIS-NX-OS-110417/114
Denial of Service; Overflow	22-03-2017	5	A Denial of Service vulnerability in the remote login functionality for Cisco	https://tools.cisco.com/security/cen	O-CIS-NX-OS-110417/115

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

			NX-OS Software running on Cisco Nexus 9000 Series Switches could allow an unauthenticated, remote attacker to cause a process used for login to terminate unexpectedly and the login attempt to fail. There is no impact to user traffic flowing through the device. The attacker could use either a Telnet or an SSH client for the remote login attempt. Affected Products: This vulnerability affects Cisco Nexus 9000 Series Switches that are running Cisco NX-OS Software and are configured to allow remote Telnet connections to the device. More Information: CSCuy25824. Known Affected Releases: 7.0(3)I3(1) 8.3(0)CV(0.342) 8.3(0)CV(0.345). Known Fixed Releases: 8.3(0)CV(0.362) 8.0(1) 7.0(3)IED5(0.19) 7.0(3)IED5(0) 7.0(3)I4(1) 7.0(3)I4(0.8) 7.0(3)I2(2e) 7.0(3)F1(1.22) 7.0(3)F1(1) 7.0(3)F1(0.230). **CVE ID: CVE-2017-3879**	ter/content/CiscoSecurityAdvisory/cisco-sa-20170315-nss1	
Bypass	22-03-2017	5	An Access-Control Filtering Mechanisms Bypass vulnerability in certain access-control filtering mechanisms on Cisco Nexus 7000 Series Switches could allow an unauthenticated, remote attacker to bypass defined traffic configured within an access control list (ACL) on the affected system. More Information: CSCtz59354. Known Affected Releases: 5.2(4) 6.1(3)S5 6.1(3)S6	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170315-cns	O-CIS-NX-OS-110417/116

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

			6.2(1.121)S0 7.2(1)D1(1) 7.3(0)ZN(0.161) 7.3(1)N1(0.1). Known Fixed Releases: 7.3(0)D1(1) 6.2(2) 6.1(5) 8.3(0)KMT(0.24) 8.3(0)CV(0.337) 7.3(1)N1(1) 7.3(0)ZN(0.210) 7.3(0)ZN(0.177) 7.3(0)ZD(0.194) 7.3(0)TSH(0.99) 7.3(0)SC(0.14) 7.3(0)RSP(0.7) 7.3(0)N1(1) 7.3(0)N1(0.193) 7.3(0)IZN(0.13) 7.3(0)IB(0.102) 7.3(0)GLF(0.44) 7.3(0)D1(0.178) 7.1(0)D1(0.14) 7.0(3)ITI2(1.6) 7.0(3)ISH1(2.13) 7.0(3)IFD6(0.78) 7.0(3)IFD6(0) 7.0(3)IDE6(0.12) 7.0(3)IDE6(0) 7.0(3)I2(1) 7.0(3)I2(0.315) 7.0(1)ZD(0.3) 7.0(0)ZD(0.84) 6.2(1.149)S0 6.2(0.285) 6.1(5.32)S0 6.1(4.97)S0 6.1(2.30)S0. **CVE ID: CVE-2017-3875**		
Digisol					
Dg-hr1400 Router Firmware DG-HR1400 is a 150Mbps Wireless Broadband Home Router.					
NA	24-03-2017	6.5	Privilege escalation vulnerability on the DIGISOL DG-HR1400 1.00.02 wireless router enables an attacker to escalate from user privilege to admin privilege just by modifying the Base64-encoded session cookie value. **CVE ID: CVE-2017-6896**	NA	O-DIG-DG-HR-110417/117
D-link					
Di-524 Firmware NA					
Cross Site Request Forgery	09-03-2017	8.5	Multiple cross-site request forgery vulnerabilities on the D-Link DI-524 Wireless Router	NA	O-D-L-DI-52-110417/118

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

			with firmware 9.01 allow remote attackers to (1) change the admin password, (2) reboot the device, or (3) possibly have unspecified other impact via crafted requests to CGI programs. **CVE ID: CVE-2017-5633**		
Google;Linux					
Android/Linux Kernel 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./The kernel is the essential center of a computer operating system, the core that provides basic services for all other parts of the operating system.					
Denial of Service; Gain Privileges	09-03-2017	6.9	Race condition in the L2TPv3 IP Encapsulation feature in the Linux kernel before 4.8.14 allows local users to gain privileges or cause a denial of service (use-after-free) by making multiple bind system calls without properly ascertaining whether a socket has the SOCK_ZAPPED status, related to net/l2tp/l2tp_ip.c and net/l2tp/l2tp_ip6.c. **CVE ID: CVE-2016-10200**	https://github.com/torvalds/linux/commit/32c231164b762dddefa13af5a0101032c70b50ef	O-GOO-ANDRO-110417/119
Hikvision					
Ds-76xxx Series Firmware;Ds-77xxx Series Firmware NA					
Denial of Service; Overflow	14-03-2017	6.8	Buffer overflow on Hikvision NVR DS-76xxNI-E1/2 and DS-77xxxNI-E4 devices before 3.4.0 allows remote authenticated users to cause a denial of service (service interruption) via a crafted HTTP request, aka the SDK issue. **CVE ID: CVE-2015-4409**	http://www.hikvision.com/En/Press-Release-details_435_i1023.html	O-HIK-DS-76-110417/120
Denial of Service; Overflow	14-03-2017	6.8	Buffer overflow on Hikvision NVR DS-76xxNI-E1/2 and DS-77xxxNI-E4 devices before 3.4.0 allows remote authenticated users to cause a	http://www.hikvision.com/En/Press-Release-details_435_	O-HIK-DS-76-110417/121

			denial of service (service interruption) via a crafted HTTP request, aka the ISAPI issue. **CVE ID: CVE-2015-4408**	i1023.html	
Denial of Service; Overflow	14-03-2017	6.8	Buffer overflow on Hikvision NVR DS-76xxNI-E1/2 and DS-77xxxNI-E4 devices before 3.4.0 allows remote authenticated users to cause a denial of service (service interruption) via a crafted HTTP request, aka the PSIA issue. **CVE ID: CVE-2015-4407**	http://www.hikvision.com/En/Press-Release-details_435_i1023.html	O-HIK-DS-76-110417/122
Huawei					
Ar3200 Firmware NA					
Denial of Service; Execute Code	27-03-2017	10	Huawei AR3200 routers with software before V200R007C00SPC600 allow remote attackers to cause a denial of service or execute arbitrary code via a crafted packet. **CVE ID: CVE-2016-6206**	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20160713-01-router-en	O-HUA-AR320-110417/123
Mate S Firmware;P8 Firmware NA					
Denial of Service	27-03-2017	7.1	The ION driver in Huawei P8 smartphones with software GRA-TL00 before GRA-TL00C01B230, GRA-CL00 before GRA-CL00C92B230, GRA-CL10 before GRA-CL10C92B230, GRA-UL00 before GRA-UL00C00B230, and GRA-UL10 before GRA-UL10C00B230 and Mate S smartphones with software CRR-TL00 before CRR-TL00C01B160SP01, CRR-UL00 before CRR-UL00C00B160, and CRR-CL00 before CRR-CL00C92B161 allows remote	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20160105-01-smartphone-en	O-HUA-MATE -110417/124

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

			attackers to cause a denial of service (crash) via a crafted application. **CVE ID: CVE-2015-8678**		
Iball					
Baton 150m Wireless-n Router Firmware NA					
Bypass	15-03-2017	5	iball Baton 150M iB-WRA150N v1 00000001 1.2.6 build 110401 Rel.47776n devices are prone to an authentication bypass vulnerability that allows remote attackers to view and modify administrative router settings by reading the HTML source code of the password.cgi file. **CVE ID: CVE-2017-6558**	NA	O-IBA-BATON-110417/125
IBM					
Advanced Management Module Firmware NA					
Cross Site Scripting	15-03-2017	4.3	Document Object Model-(DOM) based cross-site scripting vulnerability in the Advanced Management Module (AMM) versions earlier than 66Z of Lenovo IBM BladeCenter HS22, HS22V, HS23, HS23E, HX5 allows an unauthenticated attacker with access to the AMM's IP address to send a crafted URL that could inject a malicious script to access a user's AMM data such as cookies or other session information. **CVE ID: CVE-2016-8232**	https://support.lenovo.com/us/en/product_security/LEN-5700	O-IBM-ADVAN-110417/126
Juniper					
Junos Space Junos Space is a comprehensive Network Management Solution that simplifies and automates management of Juniper's switching, routing, and security devices.					
Denial of Service	22-03-2017	4	XML entity injection in Junos Space before 15.2R2 allows attackers to cause a denial of service.	https://kb.juniper.net/InfoCenter/index?page=	O-JUN-JUNOS-110417/127

			CVE ID: CVE-2016-4931	content&id=JSA10760	
Cross Site Scripting	22-03-2017	4.3	Cross-site scripting (XSS) vulnerability in Junos Space before 15.2R2 allows remote attackers to steal sensitive information or perform certain administrative actions. **CVE ID: CVE-2016-4930**	https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10760	O-JUN-JUNOS-110417/128
Execute Code	22-03-2017	9	Command injection vulnerability in Junos Space before 15.2R2 allows attackers to execute arbitrary code as a root user. **CVE ID: CVE-2016-4929**	https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10760	O-JUN-JUNOS-110417/129
Cross Site Request Forgery	22-03-2017	6.8	Cross site request forgery vulnerability in Junos Space before 15.2R2 allows remote attackers to perform certain administrative actions on Junos Space. **CVE ID: CVE-2016-4928**	https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10760	O-JUN-JUNOS-110417/130
NA	22-03-2017	6.8	Insufficient validation of SSH keys in Junos Space before 15.2R2 allows man-in-the-middle (MITM) type of attacks while a Space device is communicating with managed devices. **CVE ID: CVE-2016-4927**	https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10760	O-JUN-JUNOS-110417/131
NA	22-03-2017	7.5	Insufficient authentication vulnerability in Junos Space before 15.2R2 allows remote network based users with access to Junos Space web interface to perform certain administrative tasks without authentication. **CVE ID: CVE-2016-4926**	https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10760	O-JUN-JUNOS-110417/132
Lenovo					
Thinkserver Firmware NA					
NA	09-03-2017	5	Reset to default settings may occur in Lenovo ThinkServer TSM RD350, RD450, RD550,	https://support.lenovo.com/us/en/	O-LEN-THINK-110417/133

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

			RD650, TD350 during a prolonged broadcast storm in TSM versions earlier than 3.77. **CVE ID: CVE-2016-8236**	solutions/LEN-9307	
Linux					
Linux Kernel The kernel is the essential center of a computer operating system, the core that provides basic services for all other parts of the operating system.					
Denial of Service	15-03-2017	6.9	Race condition in kernel/ucount.c in the Linux kernel through 4.10.2 allows local users to cause a denial of service (use-after-free and system crash) or possibly have unspecified other impact via crafted system calls that leverage certain decrement behavior that causes incorrect interaction between put_ucounts and get_ucounts. **CVE ID: CVE-2017-6874**	http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=040757f738e13caaa9c5078bca79aa97e11dde88	O-LIN-LINUX-110417/134
Denial of Service; Gain Privileges	13-03-2017	7.2	Race condition in drivers/tty/n_hdlc.c in the Linux kernel through 4.10.1 allows local users to gain privileges or cause a denial of service (double free) by setting the HDLC line discipline. **CVE ID: CVE-2017-2636**	https://bugzilla.redhat.com/show_bug.cgi?id=1428319	O-LIN-LINUX-110417/135
Gain Information	14-03-2017	2.6	An information disclosure vulnerability in the kernel USB gadget driver could enable a local malicious application to access data outside of its permission levels. This issue is rated as Moderate because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.18. Android ID: A-31614969. **CVE ID: CVE-2017-0537**	NA	O-LIN-LINUX-110417/136

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

Gain Information	14-03-2017	2.6	An information disclosure vulnerability in the Synaptics touchscreen driver could enable a local malicious application to access data outside of its permission levels. This issue is rated as Moderate because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-33555878. **CVE ID: CVE-2017-0536**	NA	O-LIN-LINUX-110417/137
Gain Information	14-03-2017	2.6	An information disclosure vulnerability in the HTC sound codec driver could enable a local malicious application to access data outside of its permission levels. This issue is rated as Moderate because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10. Android ID: A-33547247. **CVE ID: CVE-2017-0535**	NA	O-LIN-LINUX-110417/138
Gain Information	13-03-2017	2.6	An information disclosure vulnerability in the Qualcomm video driver could enable a local malicious application to access data outside of its permission levels. This issue is rated as Moderate because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.18. Android ID: A-32508732. References: QC-CR#1088206. **CVE ID: CVE-2017-0534**	https://source.codeaurora.org/quic/la/kernel/msm-3.18/commit/?id=e3af5e89426f1c8d4e703d415eff5435b925649f	O-LIN-LINUX-110417/139
Gain Information	13-03-2017	2.6	An information disclosure vulnerability in the Qualcomm video driver could enable a	https://source.codeaurora.org/quic/	O-LIN-LINUX-110417/140

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

			local malicious application to access data outside of its permission levels. This issue is rated as Moderate because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.18. Android ID: A-32509422. References: QC-CR#1088206. **CVE ID: CVE-2017-0533**	la/kernel/msm-3.18/commit/?id=e3af5e89426f1c8d4e703d415eff5435b925649f	
Gain Information	13-03-2017	2.6	An information disclosure vulnerability in the Qualcomm Wi-Fi driver could enable a local malicious application to access data outside of its permission levels. This issue is rated as Moderate because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-32877245. References: QC-CR#1087469. **CVE ID: CVE-2017-0531**	https://source.codeaurora.org/quic/la/kernel/msm-3.18/commit/?id=530f3a0fd837ed105eddaf99810bc13d97dc4302	O-LIN-LINUX-110417/141
Execute Code; Bypass	13-03-2017	9.3	An elevation of privilege vulnerability in the kernel security subsystem could enable a local malicious application to to execute code in the context of a privileged process. This issue is rated as High because it is a general bypass for a kernel level defense in depth or exploit mitigation technology. Product: Android. Versions: Kernel-3.18. Android ID: A-33351919. **CVE ID: CVE-2017-0528**		O-LIN-LINUX-110417/142
Execute Code	09-03-2017	7.6	An elevation of privilege vulnerability in the HTC Sensor Hub Driver could enable a local malicious application to execute	https://source.android.com/security/bulletin/01-03-	O-LIN-LINUX-110417/143

			arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-33899318. **CVE ID: CVE-2017-0527**	2017.html	
Microsoft					
Windows Microsoft Windows (or simply Windows) is a metafamily of graphical operating systems developed, marketed, and sold by Microsoft.					
Gain Privileges	24-03-2017	7.2	The kernel-mode drivers in Microsoft Windows 10 Gold and 1511 allow local users to gain privileges via a crafted application, aka "Win32k Elevation of Privilege Vulnerability." This vulnerability is different from those described in CVE ID: CVE-2017-0024, CVE ID: CVE-2017-0026, CVE ID: CVE-2017-0056, CVE ID: CVE-2017-0078, CVE ID: CVE-2017-0079, CVE ID: CVE-2017-0080, and CVE ID: CVE-2017-0081. **CVE ID: CVE-2017-0082**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE ID: CVE-2017-0082	O-MIC-WINDO-110417/144
Overflow; Gain Privileges	20-03-2017	4.6	Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2; 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 let attackers with access to targets systems gain privileges when Windows fails to properly validate buffer lengths, aka "Windows Elevation of Privilege Vulnerability."	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE ID: CVE-2017-0102	O-MIC-WINDO-110417/145

			CVE ID: CVE-2017-0102		
Gain Privileges	21-03-2017	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." This vulnerability is different from those described in CVE ID: CVE-2017-0024, CVE ID: CVE-2017-0026, CVE ID: CVE-2017-0078, CVE ID: CVE-2017-0079, CVE ID: CVE-2017-0080, CVE ID: CVE-2017-0081, CVE ID: CVE-2017-0082. **CVE ID: CVE-2017-0056**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE ID: CVE-2017-0056	O-MIC-WINDO-110417/146
Gain Information	23-03-2017	4.3	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 1607, and Windows Server 2016 allows remote attackers to obtain sensitive information from process memory via a crafted web site, aka "Uniscribe Information Disclosure Vulnerability." CVE ID: CVE-2017-0085, CVE ID: CVE-2017-0091, CVE ID: CVE-2017-0092, CVE ID: CVE-2017-0111, CVE ID: CVE-2017-0112, CVE ID: CVE-2017-0113, CVE ID: CVE-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE ID: CVE-2017-0121	O-MIC-WINDO-110417/147

			2017-0114, CVE ID: CVE-2017-0115, CVE ID: CVE-2017-0116, CVE ID: CVE-2017-0117, CVE ID: CVE-2017-0118, CVE ID: CVE-2017-0119, CVE ID: CVE-2017-0120, CVE ID: CVE-2017-0122, CVE ID: CVE-2017-0123, CVE ID: CVE-2017-0124, CVE ID: CVE-2017-0125, CVE ID: CVE-2017-0126, CVE ID: CVE-2017-0127, and CVE ID: CVE-2017-0128. **CVE ID: CVE-2017-0121**		
Gain Information	23-03-2017	4.3	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 1607, and Windows Server 2016 allows remote attackers to obtain sensitive information from process memory via a crafted web site, aka "Uniscribe Information Disclosure Vulnerability." CVE ID: CVE-2017-0085, CVE ID: CVE-2017-0091, CVE ID: CVE-2017-0092, CVE ID: CVE-2017-0111, CVE ID: CVE-2017-0112, CVE ID: CVE-2017-0113, CVE ID: CVE-2017-0114, CVE ID: CVE-2017-0115, CVE ID: CVE-2017-0116, CVE ID: CVE-2017-0117, CVE ID: CVE-2017-0119, CVE ID: CVE-2017-0120, CVE ID: CVE-2017-0121, CVE ID: CVE-2017-0122, CVE ID: CVE-2017-0123, CVE ID: CVE-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE ID: CVE-2017-0118	O-MIC-WINDO-110417/148

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

			2017-0124, CVE ID: CVE-2017-0125, CVE ID: CVE-2017-0126, CVE ID: CVE-2017-0127, and CVE ID: CVE-2017-0128. **CVE ID: CVE-2017-0118**		
Execute Code Overflow	23-03-2017	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 1607, and Windows Server 2016 allows remote attackers to execute arbitrary code via a crafted web site, aka "Windows Uniscribe Remote Code Execution Vulnerability." This vulnerability is different from those described in CVE ID: CVE-2017-0072, CVE ID: CVE-2017-0083, CVE ID: CVE-2017-0086, CVE ID: CVE-2017-0087, CVE ID: CVE-2017-0088, CVE ID: CVE-2017-0089, and CVE ID: CVE-2017-0090. **CVE ID: CVE-2017-0084**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE ID: CVE-2017-0084	O-MIC-WINDO-110417/149
Execute Code Bypass Gain Information	24-03-2017	4.3	The Color Management Module (ICM32.dll) memory handling functionality in Windows Vista SP2; Windows Server 2008 SP2 and R2; and 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 bypass ASLR and execute code in combination with another vulnerability through a crafted website, aka	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE ID: CVE-2017-0063	O-MIC-WINDO-110417/150

			"Microsoft Color Management Information Disclosure Vulnerability." This vulnerability is different from that described in CVE ID: CVE-2017-0061. **CVE ID: CVE-2017-0063**		
XSS	24-03-2017	4.3	Microsoft Internet Information Server (IIS) in Windows Vista SP2; Windows Server 2008 SP2 and R2; 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 perform cross-site scripting and run script with local user privileges via a crafted request, aka "Microsoft IIS Server XSS Elevation of Privilege Vulnerability." **CVE ID: CVE-2017-0055**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE ID: CVE-2017-0055	O-MIC-WINDO-110417/151
Gain Privileges	24-03-2017	7.2	The kernel-mode drivers in Microsoft Windows Vista; 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." This vulnerability is different from those described in CVE ID: CVE-2017-0001, CVE ID: CVE-2017-0005, and CVE ID: CVE-2017-0047. **CVE ID: CVE-2017-0025**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE ID: CVE-2017-0025	O-MIC-WINDO-110417/152
Gain Information	24-03-2017	4.3	Microsoft XML Core Services (MSXML) in Windows 10	https://portal.msrc.micr	O-MIC-WINDO-

			Gold, 1511, and 1607; Windows 7 SP1; Windows 8.1; Windows RT 8.1; Windows Server 2008 SP2 and R2 SP1; Windows Server 2012 Gold and R2; Windows Server 2016; and Windows Vista SP2 improperly handles objects in memory, allowing attackers to test for files on disk via a crafted web site, aka "Microsoft XML Information Disclosure Vulnerability." **CVE ID: CVE-2017-0022**	osoft.com/en-US/security-guidance/advisory/CVE ID: CVE-2017-0022	110417/153
Gain Information	20-03-2017	4.3	The Graphics Device Interface (GDI) 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; and Windows 10 Gold, 1511, and 1607 allows remote attackers to obtain sensitive information from process memory via a crafted web site, aka "Windows GDIGain Informationrmation Disclosure Vulnerability." This vulnerability is different from those described in CVE ID: CVE-2017-0060 and CVE ID: CVE-2017-0062. **CVE ID: CVE-2017-0073**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE ID: CVE-2017-0073	O-MIC-WINDO-110417/154
Gain Information	21-03-2017	1.9	The Graphics Device Interface (GDI) 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; and Windows 10 Gold, 1511, and 1607 allows remote attackers to obtain sensitive information from process	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE ID: CVE-2017-0062	O-MIC-WINDO-110417/155

			memory via a crafted web site, aka "GDIGain Informationrmation Disclosure Vulnerability." This vulnerability is different from those described in CVE ID: CVE-2017-0060 and CVE ID: CVE-2017-0073. **CVE ID: CVE-2017-0062**		
Gain Information	21-03-2017	1.9	The Graphics Device Interface (GDI) 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; and Windows 10 Gold, 1511, and 1607 allows remote attackers to obtain sensitive information from process memory via a crafted web site, aka "GDIGain Informationrmation Disclosure Vulnerability." This vulnerability is different from those described in CVE ID: CVE-2017-0060 and CVE ID: CVE-2017-0062. **CVE ID: CVE-2017-0060**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE ID: CVE-2017-0060	O-MIC-WINDO-110417/156
Gain Privileges	21-03-2017	7.2	The Graphics Device Interface (GDI) 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; and Windows 10 Gold, 1511, and 1607 allows local users to gain privileges via a crafted application, aka "Windows GDI Elevation of Privilege Vulnerability." This vulnerability is different from those described in CVE ID: CVE-2017-0001, CVE ID: CVE-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE ID: CVE-2017-0047	O-MIC-WINDO-110417/157

			2017-0005 and CVE ID: CVE-2017-0025. **CVE ID: CVE-2017-0047**		
Gain Privileges	23-03-2017	7.2	The Graphics Device Interface (GDI) 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; and Windows 10 Gold, 1511, and 1607 allows local users to gain privileges via a crafted application, aka "Windows GDI Elevation of Privilege Vulnerability." This vulnerability is different from those described in CVE ID: CVE-2017-0005, CVE ID: CVE-2017-0025, and CVE ID: CVE-2017-0047. **CVE ID: CVE-2017-0001**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE ID: CVE-2017-0001	O-MIC-WINDO-110417/158
Denial of Service	20-03-2017	2.3	Hyper-V in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and 2008 R2; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows 10 Gold, 1511, and 1607; and Windows Server 2016 allows guest OS users, running as virtual machines, to cause a denial of service via a crafted application, aka "Hyper-V Denial of Service Vulnerability." This vulnerability is different from those described in CVE ID: CVE-2017-0098, CVE ID: CVE-2017-0074, CVE ID: CVE-2017-0076, and CVE ID: CVE-2017-0097. **CVE ID: CVE-2017-0099**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE ID: CVE-2017-0099	O-MIC-WINDO-110417/159

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	20-03-2017	2.3	Hyper-V in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and 2008 R2; Windows 7 SP1; Windows 8.1; Windows Server 2012 and R2; Windows 10, 1511, and 1607; and Windows Server 2016 allows guest OS users, running as virtual machines, to cause a denial of service via a crafted application, aka "Hyper-V Denial of Service Vulnerability." This vulnerability is different from those described in CVE ID: CVE-2017-0098, CVE ID: CVE-2017-0074, CVE ID: CVE-2017-0076, and CVE ID: CVE-2017-0099. **CVE ID: CVE-2017-0097**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE ID: CVE-2017-0097	O-MIC-WINDO-110417/160
Denial of Service	20-03-2017	2.9	Hyper-V in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and 2008 R2; Windows 7 SP1; Windows 8.1; Windows Server 2012 and R2; Windows 10, 1511, and 1607; and Windows Server 2016 allows guest OS users, running as virtual machines, to cause a denial of service via a crafted application, aka "Hyper-V Denial of Service Vulnerability." This vulnerability is different from those described in CVE ID: CVE-2017-0098, CVE ID: CVE-2017-0074, CVE ID: CVE-2017-0097, and CVE ID: CVE-2017-0099. **CVE ID: CVE-2017-0076**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE ID: CVE-2017-0076	O-MIC-WINDO-110417/161
Denial of Service	20-03-2017	2.3	Hyper-V in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and 2008	https://portal.msrc.microsoft.com/e	O-MIC-WINDO-110417/162

			R2; Windows 7 SP1; Windows 8.1; Windows Server 2012 and R2; Windows 10, 1511, and 1607; and Windows Server 2016 allows guest OS users, running as virtual machines, to cause a denial of service via a crafted application, aka "Hyper-V Denial of Service Vulnerability." This vulnerability is different from those described in CVE-2017-0098, CVE-2017-0076, CVE-2017-0097, and CVE-2017-0099. **CVE ID: CVE-2017-0074**	n-US/security-guidance/advisory/CVE ID: CVE-2017-0074	
Execute Code	22-03-2017	7.4	Hyper-V in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows 10 Gold, 1511, and 1607; and Windows Server 2016 allows guest OS users to execute arbitrary code on the host OS via a crafted application, aka "Hyper-V Remote Code Execution Vulnerability." This vulnerability is different from that described in CVE-2017-0075. **CVE ID: CVE-2017-0109**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0109	O-MIC-WINDO-110417/163
Sagemcom					
Livebox Firmware NA					
NA	14-03-2017	7.8	Livebox 3 Sagemcom SG30_sip-fr-5.15.8.1 devices have an insufficiently large default value for the maximum IPv6 routing table size: it can be filled within minutes. An attacker can exploit this issue to render	NA	O-SAG-LIVEB-110417/164

			the affected system unresponsive, resulting in a denial-of-service condition for telephone, Internet, and TV services. **CVE ID: CVE-2017-6552**		
Suse					
Linux Enterprise Desktop; Linux Enterprise Server SUSE Linux Enterprise Desktop delivers essential office functionality affordably, and was built to coexist with other operating systems.					
Execute Code	27-03-2017	7.2	A code injection in the supportconfig data collection tool in supportutils in SUSE Linux Enterprise Server 12 and 12-SP1 and SUSE Linux Enterprise Desktop 12 and 12-SP1 could be used by local attackers to execute code as the user running supportconfig (usually root). **CVE ID: CVE-2016-1602**	http://lists.suse.com/pipermail/sle-security-updates/2016-June/002096.html	O-SUS-LINUX-110417/165