Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Application (A)					
Adobe					
Acrobat; Acrobat Dc; Acrobat Reader Dc; Reader Adobe Acrobat is a family of application software and Web services developed by Adobe Systems to view, create, manipulate, print and manage files in Portable Document Format (PDF).					
Execute Code; Overflow; Memory Corruption	10-01-2017	9.3	Adobe Acrobat Reader versions 15.020.20042 and earlier, 15.006.30244 and earlier, 11.0.18 and earlier have an exploitable memory corruption vulnerability in the XFA engine related to a form's structure and organization. Successful exploitation could lead to arbitrary code execution. **Reference: CVE-2017-2967**	https://helpx.adobe.com/security/products/acrobat/apsb17-01.html	A-ADO-ACROB-190117/01
Execute Code; Overflow	10-01-2017	9.3	Adobe Acrobat Reader versions 15.020.20042 and earlier, 15.006.30244 and earlier, 11.0.18 and earlier have an exploitable heap overflow vulnerability in the image conversion engine related to parsing malformed TIFF segments. Successful exploitation could lead to arbitrary code execution. **Reference: CVE-2017-2966**	https://helpx.adobe.com/security/products/acrobat/apsb17-01.html	A-ADO-ACROB-190117/02
Execute Code; Overflow; Memory Corruption	10-01-2017	9.3	Adobe Acrobat Reader versions 15.020.20042 and earlier, 15.006.30244 and earlier, 11.0.18 and earlier have an exploitable memory corruption vulnerability in the image conversion engine, related to TIFF file parsing. Successful exploitation could lead to arbitrary code execution. **Reference: CVE-2017-2965**	https://helpx.adobe.com/security/products/acrobat/apsb17-01.html	A-ADO-ACROB-190117/03

Execute Code; Overflow; Memory Corruption	10-01-2017	9.3	Adobe Acrobat Reader versions 15.020.20042 and earlier, 15.006.30244 and earlier, 11.0.18 and earlier have an exploitable memory corruption vulnerability in the image conversion engine, related to the parsing of JPEG EXIF metadata. Successful exploitation could lead to arbitrary code execution. **Reference: CVE-2017-2964**	https://helpx.adobe.com/security/products/acrobat/apsb17-01.html	A-ADO-ACROB-190117/04
Execute Code; Overflow; Memory Corruption	10-01-2017	9.3	Adobe Acrobat Reader versions 15.020.20042 and earlier, 15.006.30244 and earlier, 11.0.18 and earlier have an exploitable memory corruption vulnerability in the image conversion engine, related to handling of the color profile in a TIFF file. Successful exploitation could lead to arbitrary code execution. **Reference: CVE-2017-2963**	https://helpx.adobe.com/security/products/acrobat/apsb17-01.html	A-ADO-ACROB-190117/05
Execute Code	10-01-2017	9.3	Adobe Acrobat Reader versions 15.020.20042 and earlier, 15.006.30244 and earlier, 11.0.18 and earlier have an exploitable type confusion vulnerability in the XSLT engine related to localization functionality. Successful exploitation could lead to arbitrary code execution. **Reference: CVE-2017-2962**	https://helpx.adobe.com/security/products/acrobat/apsb17-01.html	A-ADO-ACROB-190117/06
Execute Code	10-01-2017	9.3	Adobe Acrobat Reader versions 15.020.20042 and earlier, 15.006.30244 and earlier, 11.0.18 and earlier have an exploitable use after free vulnerability in the XFA engine, related to validation functionality. Successful exploitation could lead to arbitrary code execution. **Reference: CVE-2017-2961**	https://helpx.adobe.com/security/products/acrobat/apsb17-01.html	A-ADO-ACROB-190117/07

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; Memory Corruption	10-01-2017	9.3	Adobe Acrobat Reader versions 15.020.20042 and earlier, 15.006.30244 and earlier, 11.0.18 and earlier have an exploitable memory corruption vulnerability in the image conversion engine, related to parsing of EXIF metadata. Successful exploitation could lead to arbitrary code execution. **Reference: CVE-2017-2960**	https://helpx.adobe.com/security/products/acrobat/apsb17-01.html	A-ADO-ACROB-190117/08
Execute Code; Overflow	10-01-2017	9.3	Adobe Acrobat Reader versions 15.020.20042 and earlier, 15.006.30244 and earlier, 11.0.18 and earlier have an exploitable heap overflow vulnerability in the image conversion engine, related to parsing of color profile metadata. Successful exploitation could lead to arbitrary code execution. **Reference: CVE-2017-2959**	https://helpx.adobe.com/security/products/acrobat/apsb17-01.html	A-ADO-ACROB-190117/09
Execute Code	10-01-2017	9.3	Adobe Acrobat Reader versions 15.020.20042 and earlier, 15.006.30244 and earlier, 11.0.18 and earlier have an exploitable use after free vulnerability in the JavaScript engine. Successful exploitation could lead to arbitrary code execution. **Reference: CVE-2017-2958**	https://helpx.adobe.com/security/products/acrobat/apsb17-01.html	A-ADO-ACROB-190117/10
Execute Code	10-01-2017	9.3	Adobe Acrobat Reader versions 15.020.20042 and earlier, 15.006.30244 and earlier, 11.0.18 and earlier have an exploitable use after free vulnerability in the JavaScript engine, related to collaboration functionality. Successful exploitation could lead to arbitrary code execution. **Reference: CVE-2017-2957**	https://helpx.adobe.com/security/products/acrobat/apsb17-01.html	A-ADO-ACROB-190117/11
Execute Code	10-01-2017	9.3	Adobe Acrobat Reader versions	https://hel	A-ADO-

			15.020.20042 and earlier, 15.006.30244 and earlier, 11.0.18 and earlier have an exploitable use after free vulnerability in the JavaScript engine, related to manipulation of the navigation pane. Successful exploitation could lead to arbitrary code execution. **Reference: CVE-2017-2956**	px.adobe.com/security/products/acrobat/apsb17-01.html	ACROB-190117/12
Execute Code	10-01-2017	9.3	Adobe Acrobat Reader versions 15.020.20042 and earlier, 15.006.30244 and earlier, 11.0.18 and earlier have an exploitable use after free vulnerability in the JavaScript engine. Successful exploitation could lead to arbitrary code execution. **Reference: CVE-2017-2955**	https://helpx.adobe.com/security/products/acrobat/apsb17-01.html	A-ADO-ACROB-190117/13
Execute Code; Overflow; Memory Corruption	10-01-2017	9.3	Adobe Acrobat Reader versions 15.020.20042 and earlier, 15.006.30244 and earlier, 11.0.18 and earlier have an exploitable memory corruption vulnerability in the image conversion module when handling malformed TIFF images. Successful exploitation could lead to arbitrary code execution. **Reference: CVE-2017-2954**	https://helpx.adobe.com/security/products/acrobat/apsb17-01.html	A-ADO-ACROB-190117/14
Execute Code; Overflow; Memory Corruption	10-01-2017	9.3	Adobe Acrobat Reader versions 15.020.20042 and earlier, 15.006.30244 and earlier, 11.0.18 and earlier have an exploitable memory corruption vulnerability in the image conversion module when processing a TIFF image. Successful exploitation could lead to arbitrary code execution. **Reference: CVE-2017-2953**	https://helpx.adobe.com/security/products/acrobat/apsb17-01.html	A-ADO-ACROB-190117/15
Execute Code; Overflow	10-01-2017	9.3	Adobe Acrobat Reader versions 15.020.20042 and earlier,	https://helpx.adobe.co	A-ADO-ACROB-

			15.006.30244 and earlier, 11.0.18 and earlier have an exploitable buffer overflow / underflow vulnerability in the image conversion module related to parsing tags in TIFF files. Successful exploitation could lead to arbitrary code execution. **Reference: CVE-2017-2952**	m/security /products/ acrobat/ap sb17-01.html	190117/16
Execute Code	10-01-2017	9.3	Adobe Acrobat Reader versions 15.020.20042 and earlier, 15.006.30244 and earlier, 11.0.18 and earlier have an exploitable use after free vulnerability in the XFA engine, related to sub-form functionality. Successful exploitation could lead to arbitrary code execution. **Reference: CVE-2017-2951**	https://helpx.adobe.com/security/products/acrobat/apsb17-01.html	A-ADO-ACROB-190117/17
Execute Code	10-01-2017	9.3	Adobe Acrobat Reader versions 15.020.20042 and earlier, 15.006.30244 and earlier, 11.0.18 and earlier have an exploitable use after free vulnerability in the XFA engine, related to layout functionality. Successful exploitation could lead to arbitrary code execution. **Reference: CVE-2017-2950**	https://helpx.adobe.com/security/products/acrobat/apsb17-01.html	A-ADO-ACROB-190117/18
Execute Code; Overflow	10-01-2017	9.3	Adobe Acrobat Reader versions 15.020.20042 and earlier, 15.006.30244 and earlier, 11.0.18 and earlier have an exploitable heap overflow vulnerability in the XSLT engine. Successful exploitation could lead to arbitrary code execution. **Reference: CVE-2017-2949**	https://helpx.adobe.com/security/products/acrobat/apsb17-01.html	A-ADO-ACROB-190117/19
Execute Code; Overflow	10-01-2017	9.3	Adobe Acrobat Reader versions 15.020.20042 and earlier, 15.006.30244 and earlier, 11.0.18 and earlier have an exploitable buffer overflow /	https://helpx.adobe.com/security/products/acrobat/ap	A-ADO-ACROB-190117/20

			underflow vulnerability in the XFA engine. Successful exploitation could lead to arbitrary code execution. **Reference: CVE-2017-2948**	sb17-01.html	
Bypass	10-01-2017	4.3	Adobe Acrobat Reader versions 15.020.20042 and earlier, 15.006.30244 and earlier, 11.0.18 and earlier have a security bypass vulnerability when manipulating Form Data Format (FDF). **Reference: CVE-2017-2947**	https://helpx.adobe.com/security/products/acrobat/apsb17-01.html	A-ADO-ACROB-190117/21
Execute Code; Overflow	10-01-2017	9.3	Adobe Acrobat Reader versions 15.020.20042 and earlier, 15.006.30244 and earlier, 11.0.18 and earlier have an exploitable heap overflow vulnerability when parsing the segment for storing non-graphic information. Successful exploitation could lead to arbitrary code execution. **Reference: CVE-2017-2946**	https://helpx.adobe.com/security/products/acrobat/apsb17-01.html	A-ADO-ACROB-190117/22
Execute Code; Overflow	10-01-2017	9.3	Adobe Acrobat Reader versions 15.020.20042 and earlier, 15.006.30244 and earlier, 11.0.18 and earlier have an exploitable heap overflow vulnerability when parsing TIFF image files. Successful exploitation could lead to arbitrary code execution. **Reference: CVE-2017-2945**	https://helpx.adobe.com/security/products/acrobat/apsb17-01.html	A-ADO-ACROB-190117/23
Execute Code; Overflow; Memory Corruption	10-01-2017	9.3	Adobe Acrobat Reader versions 15.020.20042 and earlier, 15.006.30244 and earlier, 11.0.18 and earlier have an exploitable memory corruption vulnerability when parsing crafted TIFF image files. Successful exploitation could lead to arbitrary code execution. **Reference: CVE-2017-2944**	https://helpx.adobe.com/security/products/acrobat/apsb17-01.html	A-ADO-ACROB-190117/24

Execute Code; Overflow; Memory Corruption	10-01-2017	9.3	Adobe Acrobat Reader versions 15.020.20042 and earlier, 15.006.30244 and earlier, 11.0.18 and earlier have an exploitable memory corruption vulnerability when processing tags in TIFF images. Successful exploitation could lead to arbitrary code execution. **Reference: CVE-2017-2943**	https://helpx.adobe.com/security/products/acrobat/apsb17-01.html	A-ADO-ACROB-190117/25
Execute Code; Overflow	10-01-2017	9.3	Adobe Acrobat Reader versions 15.020.20042 and earlier, 15.006.30244 and earlier, 11.0.18 and earlier have an exploitable heap overflow vulnerability when processing TIFF image data. Successful exploitation could lead to arbitrary code execution. **Reference: CVE-2017-2942**	https://helpx.adobe.com/security/products/acrobat/apsb17-01.html	A-ADO-ACROB-190117/26
Execute Code; Overflow; Memory Corruption	10-01-2017	9.3	Adobe Acrobat Reader versions 15.020.20042 and earlier, 15.006.30244 and earlier, 11.0.18 and earlier have an exploitable memory corruption vulnerability when processing Compact Font Format data. Successful exploitation could lead to arbitrary code execution. **Reference: CVE-2017-2941**	https://helpx.adobe.com/security/products/acrobat/apsb17-01.html	A-ADO-ACROB-190117/27
Execute Code; Overflow; Memory Corruption	10-01-2017	9.3	Adobe Acrobat Reader versions 15.020.20042 and earlier, 15.006.30244 and earlier, 11.0.18 and earlier have an exploitable memory corruption vulnerability when processing JPEG 2000 files. Successful exploitation could lead to arbitrary code execution. **Reference: CVE-2017-2940**	https://helpx.adobe.com/security/products/acrobat/apsb17-01.html	A-ADO-ACROB-190117/28
Execute Code; Overflow; Memory Corruption	10-01-2017	9.3	Adobe Acrobat Reader versions 15.020.20042 and earlier, 15.006.30244 and earlier, 11.0.18 and earlier have an exploitable memory corruption	https://helpx.adobe.com/security/products/acrobat/ap	A-ADO-ACROB-190117/29

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

			vulnerability when processing a malformed cross-reference table. Successful exploitation could lead to arbitrary code execution. **Reference: CVE-2017-2939**	sb17-01.html	
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.					
Bypass	10-01-2017	7.5	Adobe Flash Player versions 24.0.0.186 and earlier have a security bypass vulnerability related to handling TCP connections. **Reference: CVE-2017-2938**	https://helpx.adobe.com/security/products/flash-player/apsb17-02.html	A-ADO-FLASH-190117/30
Execute Code	10-01-2017	10	Adobe Flash Player versions 24.0.0.186 and earlier have an exploitable use after free vulnerability in the ActionScript FileReference class, when using class inheritance. Successful exploitation could lead to arbitrary code execution. **Reference: CVE-2017-2937**	https://helpx.adobe.com/security/products/flash-player/apsb17-02.html	A-ADO-FLASH-190117/31
Execute Code	10-01-2017	10	Adobe Flash Player versions 24.0.0.186 and earlier have an exploitable use after free vulnerability in the ActionScript FileReference class. Successful exploitation could lead to arbitrary code execution. **Reference: CVE-2017-2936**	https://helpx.adobe.com/security/products/flash-player/apsb17-02.html	A-ADO-FLASH-190117/32
Execute Code; Overflow	10-01-2017	10	Adobe Flash Player versions 24.0.0.186 and earlier have an exploitable heap overflow vulnerability when processing the Flash Video container file format. Successful exploitation could lead to arbitrary code execution. **Reference: CVE-2017-2935**	https://helpx.adobe.com/security/products/flash-player/apsb17-02.html	A-ADO-FLASH-190117/33
Execute Code; Overflow	10-01-2017	10	Adobe Flash Player versions 24.0.0.186 and earlier have an	https://helpx.adobe.co	A-ADO-FLASH-

			exploitable heap overflow vulnerability when parsing Adobe Texture Format files. Successful exploitation could lead to arbitrary code execution. **Reference: CVE-2017-2934**	m/security /products/flash-player/apsb17-02.html	190117/34
Execute Code; Overflow	10-01-2017	10	Adobe Flash Player versions 24.0.0.186 and earlier have an exploitable heap overflow vulnerability related to texture compression. Successful exploitation could lead to arbitrary code execution. **Reference: CVE-2017-2933**	https://helpx.adobe.com/security /products/flash-player/apsb17-02.html	A-ADO-FLASH-190117/35
Execute Code	10-01-2017	10	Adobe Flash Player versions 24.0.0.186 and earlier have an exploitable use after free vulnerability in the ActionScript MovieClip class. Successful exploitation could lead to arbitrary code execution. **Reference: CVE-2017-2932**	https://helpx.adobe.com/security /products/flash-player/apsb17-02.html	A-ADO-FLASH-190117/36
Apache					
Storm Apache Storm is a free and open source distributed real-time computation system.					
Execute Code	13-01-2017	10	The UI daemon in Apache Storm 0.10.0 before 0.10.0-beta1 allows remote attackers to execute arbitrary code via unspecified vectors. **Reference: CVE-2015-3188**	NA	A-APA-STORM-190117/37
Awebsupport					
Aweb Cart Watching System For Virtuemart NA					
Execute Code; SQL Injection	03-01-2017	7.5	SQL injection vulnerability in the "aWeb Cart Watching System for Virtuemart" extension before 2.6.1 for Joomla! allows remote attackers to execute arbitrary SQL commands via vectors involving categorysearch and smartSearch. **Reference: CVE-2016-10114**	NA	A-AWE-AWEB - 190117/38

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

B2evolution					
B2evolution b2evolution is a content and community management system written in PHP and backed by a MySQL database.					
Cross Site Scripting	15-01-2017	3.5	Multiple cross-site scripting (XSS) vulnerabilities in the file types table in b2evolution through 6.8.3 allow remote authenticated users to inject arbitrary web script or HTML via a .swf file in a (1) comment frame or (2) avatar frame. **Reference: CVE-2017-5494**	https://github.com/b2evolution/b2evolution/commit/261dbd5b294e707af766691e65a177a290314a6e	A-B2E-B2EVO-190117/39
Bluestacks					
Bluestacks Bluestacks is an American technology company that produces the BlueStacks App Player and other cloud-based cross-platform products.					
NA	06-01-2017	7.2	A local privilege escalation vulnerability exists in BlueStacks App Player. The BlueStacks App Player installer creates a registry key with weak permissions that allows users to execute arbitrary programs with SYSTEM privileges. **Reference: CVE-2016-4288**	NA	A-BLU-BLUES-190117/40
Borg					
Borg The main goal of Borg is to provide an efficient and secure way to backup data.					
NA	02-01-2017	5	Borg (aka BorgBackup) before 1.0.9 has a flaw in the way duplicate archive names were processed during manifest recovery, potentially allowing an attacker to overwrite an archive. **Reference: CVE-2016-10100**	http://borgbackup.readthedocs.io/en/stable/changes.html#pre-1-0-9-manifest-spoofing-vulnerability	A-BOR-BORG-190117/41
NA	02-01-2017	5	Borg (aka BorgBackup) before 1.0.9 has a flaw in the cryptographic protocol used to	http://borgbackup.readthedocs.io	A-BOR-BORG-190117/42

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

			authenticate the manifest (list of archives), potentially allowing an attacker to spoof the list of archives. **Reference: CVE-2016-10099**	/en/stable/changes.html#pre-1-0-9-manifest-spoofing-vulnerability	
Brocade					
Network Advisor Brocade Network Advisor greatly simplifies daily operations while improving the performance and reliability of the overall Storage Area Network (SAN) and IP networking environment. This software management tool offers flexible and proactive network performance analysis, in addition to network configuration change deployment and monitoring for compliance.					
Directory Traversal	14-01-2017	5	A Directory Traversal vulnerability in CliMonitorReportServlet in the Brocade Network Advisor versions released prior to and including 14.0.2 could allow remote attackers to read arbitrary files including files with sensitive user information. **Reference: CVE-2016-8207**	https://www.brocade.com/content/dam/common/documents/content-types/security-bulletin/brocade-security-advisory-2016-180.htm	A-BRO-NETWO-190117/43
Directory Traversal	14-01-2017	6.4	A Directory Traversal vulnerability in servlet SoftwareImageUpload in the Brocade Network Advisor versions released prior to and including 14.0.2 could allow remote attackers to write to arbitrary files, and consequently delete the files. **Reference: CVE-2016-8206**	https://www.brocade.com/content/dam/common/documents/content-types/security-bulletin/brocade-security-advisory-2016-179.htm	A-BRO-NETWO-190117/44

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

Directory Traversal	14-01-2017	10	A Directory Traversal vulnerability in DashboardFileReceiveServlet in the Brocade Network Advisor versions released prior to and including 14.0.2 could allow remote attackers to upload a malicious file in a section of the file system where it can be executed. **Reference: CVE-2016-8205**	https://www.brocade.com/content/dam/common/documents/content-types/security-bulletin/brocade-security-advisory-2016-178.htm	A-BRO-NETWO-190117/45
Directory Traversal	14-01-2017	10	A Directory Traversal vulnerability in FileReceiveServlet in the Brocade Network Advisor versions released prior to and including 14.0.2 could allow remote attackers to upload a malicious file in a section of the file system where it can be executed. **Reference: CVE-2016-8204**	https://www.brocade.com/content/dam/common/documents/content-types/security-bulletin/brocade-security-advisory-2016-177.htm	A-BRO-NETWO-190117/46
Call-cc					
Chicken CHICKEN is a compiler for the Scheme programming language.					
Denial of Service	10-01-2017	5	The "process-execute" and "process-spawn" procedures did not free memory correctly when the execve() call failed, resulting in a memory leak. This could be abused by an attacker to cause resource exhaustion or a denial of service. This affects all releases of CHICKEN up to and including 4.11 (it will be fixed in 4.12 and 5.0, which are not yet released).	NA	A-CAL-CHICK-190117/47

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-2016-6831		
Overflow	10-01-2017	7.5	The "process-execute" and "process-spawn" procedures in CHICKEN Scheme used fixed-size buffers for holding the arguments and environment variables to use in its execve() call. This would allow user-supplied argument/environment variable lists to trigger a buffer overrun. This affects all releases of CHICKEN up to and including 4.11 (it will be fixed in 4.12 and 5.0, which are not yet released). **Reference: CVE-2016-6830**	NA	A-CAL-CHICK-190117/48
Http-client NA					
NA	10-01-2017	5	The "http-client" egg always used a HTTP_PROXY environment variable to determine whether HTTP traffic should be routed via a proxy, even when running as a CGI process. Under several web servers this would mean a user-supplied "Proxy" header could allow an attacker to direct all HTTP requests through a proxy (also known as a "httpoxy" attack). This affects all versions of http-client before 0.10. **Reference: CVE-2016-6287**	NA	A-CAL-HTTP--190117/49
NA	10-01-2017	5	The "spiffy-cgi-handlers" egg would convert a nonexistent "Proxy" header to the HTTP_PROXY environment variable, which would allow attackers to direct CGI programs which use this environment variable to use an attacker-specified HTTP proxy server (also known as a "httpoxy" attack). This affects all versions of spiffy-cgi-handlers before 0.5.	NA	A-CAL-HTTP--190117/50

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-2016-6286		
Codeigniter					
Codeigniter CodeIgniter is an Application Development Framework (a toolkit) for people who build web sites using PHP.					
Execute Code	12-01-2017	7.5	system/libraries/Email.php in CodeIgniter before 3.1.3 allows remote attackers to execute arbitrary code by leveraging control over the email->from field to insert sendmail command-line arguments. **Reference: CVE-2016-10131**	NA	A-COD-CODEI-190117/51
Docker					
Docker Docker is an open platform for developers and sysadmins to build, ship, and run distributed applications, whether on laptops, data center VMs, or the cloud.					
DoS	04-01-2017	4	** DISPUTED ** The SwarmKit toolkit 1.12.0 for Docker allows remote authenticated users to cause a denial of service (prevention of cluster joins) via a long sequence of join and quit actions. NOTE: the vendor disputes this issue, stating that this sequence is not "removing the state that is left by old nodes. At some point the manager obviously stops being able to accept new nodes, since it runs out of memory. Given that both for Docker swarm and for Docker Swarmkit nodes are *required* to provide a secret token (it's actually the only mode of operation), this means that no adversary can simply join nodes and exhaust manager resources. We can't do anything about a manager running out of memory and not being able to add new legitimate nodes to the system. This is merely a resource provisioning issue, and	NA	A-DOC-DOCKE-190117/52

			definitely not a CVE worthy vulnerability." **Reference: CVE-2016-6595**		
Dotclear					
Dotclear Dotclear is an open source blog publishing application distributed under the GNU GPLv2.					
NA	04-01-2017	4.3	Dotclear before 2.10.3, when the Host header is not part of the web server routing process, allows remote attackers to modify the password reset address link via the HTTP Host header. **Reference: CVE-2016-7903**	https://dotclear.org/blog/post/2016/11/01/Dotclear-2.10.3	A-DOT-DOTCL-190117/53
Execute Code	04-01-2017	6.5	Unrestricted file upload vulnerability in the fileUnzip->unzip method in Dotclear before 2.10.3 allows remote authenticated users with permissions to manage media items to execute arbitrary code by uploading a ZIP file containing a file with a crafted extension, as demonstrated by .php.txt or .php%20. **Reference: CVE-2016-7902**	https://dotclear.org/blog/post/2016/11/01/Dotclear-2.10.3	A-DOT-DOTCL-190117/54
Eclinicalworks					
Population Health eClinicalWorks is the most used Population Health Solution across all functional ACO categories according to KLAS.					
Cross Site request Forgery	10-01-2017	6.8	eClinicalWorks Population Health (CCMR) suffers from a cross-site request forgery (CSRF) vulnerability in portalUserService.jsp which allows remote attackers to hijack the authentication of content administrators for requests that could lead to the creation, modification and deletion of users, appointments and employees. **Reference: CVE-2015-4593**	NA	A-ECL-POPUL-190117/55
SQL Injection	10-01-2017	7.5	eClinicalWorks Population	NA	A-ECL-

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

			Health (CCMR) suffers from an SQL injection vulnerability in portalUserService.jsp which allows remote authenticated users to inject arbitrary malicious database commands as part of user input. **Reference: CVE-2015-4592**		POPUL-190117/56
Cross Site Scripting	10-01-2017	4.3	eClinicalWorks Population Health (CCMR) suffers from a cross site scripting vulnerability in login.jsp which allows remote unauthenticated users to inject arbitrary javascript via the strMessage parameter. **Reference: CVE-2015-4591**	NA	A-ECL-POPUL-190117/57
EMC					
Scaleio EMC ScaleIO is a software-defined solution that uses your existing hardware or EMC servers to turn existing DAS storage into shared block storage.					
NA	06-01-2017	2.1	An issue was discovered in EMC ScaleIO versions before 2.0.1.1. Incorrect permissions on the SCINI driver may allow a low-privileged local attacker to modify the configuration and render the ScaleIO Data Client (SDC) server unavailable. **Reference: CVE-2016-9869**	http://www.securityfocus.com/archive/1/539983/30/0/threaded	A-EMC-SCALE-190117/58
NA	06-01-2017	2.1	An issue was discovered in EMC ScaleIO versions before 2.0.1.1. A low-privileged local attacker may cause a denial-of-service by generating a kernel panic in the SCINI driver using IOCTL calls which may render the ScaleIO Data Client (SDC) server unavailable until the next reboot. **Reference: CVE-2016-9868**	http://www.securityfocus.com/archive/1/539983/30/0/threaded	A-EMC-SCALE-190117/59
Execute Code	06-01-2017	4.6	An issue was discovered in EMC ScaleIO versions before 2.0.1.1. A low-privileged local attacker may be able to modify the kernel	http://www.securityfocus.com/archive/1/5	A-EMC-SCALE-190117/60

			memory in the SCINI driver and may achieve code execution to escalate privileges to root on ScaleIO Data Client (SDC) servers. **Reference: CVE-2016-9867**	39983/30/0/threaded	
Exponentcms					
Exponent Cms Exponent CMS is an Open Source Content Management System, based on PHP, MySQL and the Exponent Framework.					
Execute Code	12-01-2017	7.5	Exponent CMS 2.3.9 suffers from a remote code execution vulnerability in /install/index.php. An attacker can upload an evil 'exploit.tar.gz' file to the website, then extract it by visiting '/install/index.php?install_sample=../../files/exploit', which leads to arbitrary code execution. **Reference: CVE-2016-7791**	NA	A-EXP-EXPON-190117/61
Execute Code	12-01-2017	7.5	Exponent CMS 2.3.9 suffers from a remote code execution vulnerability in /install/index.php. An attacker can upload 'php' file to the website through uploader_paste.php, then overwrite /framework/conf/config.php, which leads to arbitrary code execution. **Reference: CVE-2016-7790**	NA	A-EXP-EXPON-190117/62
F5					
Big-ip Access Policy Manager; Big-ip Advanced Firewall Manager; Big-ip Analytics; Big-ip Application Acceleration Manager; Big-ip Application Security Manager; Big-ip Domain Name System; Big-ip Global Traffic Manager; Big-ip Link Controller; Big-ip Local Traffic Manager; Big-ip Policy Enforcement Manager The BIG-IP platform is a smart evolution of Application Delivery Controller (ADC) technology.					
Denial of Service	03-01-2017	4.3	Virtual servers in F5 BIG-IP systems 11.6.1 before 11.6.1 HF1 and 12.1.x before 12.1.2, when configured to parse RADIUS messages via an iRule,	https://support.f5.com/csp/#/article/K92859602	A-F5-BIG-I-190117/63

			allow remote attackers to cause a denial of service (Traffic Management Microkernel restart) via crafted network traffic. **Reference: CVE-2016-5024**		
NA	10-01-2017	4.3	Under certain conditions for BIG-IP systems using a virtual server with an associated FastL4 profile and TCP analytics profile, a specific sequence of packets may cause the Traffic Management Microkernel (TMM) to restart. **Reference: CVE-2016-9247**	https://support.f5.com/csp/#/article/K33500120	A-F5-BIG-I-190117/64
Forgerock					
Openam OpenAM is an open source access management, entitlements and federation server platform.					
NA	02-01-2017	5	XML External Entity (XXE) Vulnerability in /SSOPOST/metaAlias/%realm%/idpv2 in OpenAM - Access Management 10.1.0 allows remote attackers to read arbitrary files via the SAMLRequest parameter. **Reference: CVE-2016-10097**	NA	A-FOR-OPENA-190117/65
Foxitsoftware					
Foxit Pdf Toolkit Foxit PDF Toolkit's suite of advanced modules provides high volume PDF creation and processing to optimize workflows.					
Denial of Service; Execute Code; Overflow; Memory Corruption	13-01-2017	6.8	Memory Corruption Vulnerability in Foxit PDF Toolkit v1.3 allows an attacker to cause Denial of Service and Remote Code Execution when the victim opens the specially crafted PDF file. The Vulnerability has been fixed in v2.0. **Reference: CVE-2017-5364**	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-FOXIT-190117/66
Reader Foxit Reader is a lightweight, fast, and secure PDF Reader capable of high-volume processing.					
Bypass; Gain	06-01-2017	4.3	A large out-of-bounds read on	NA	A-FOX-

Information			the heap vulnerability in Foxit PDF Reader can potentially be abused for information disclosure. Combined with another vulnerability, it can be used to leak heap memory layout and in bypassing ASLR. **Reference: CVE-2016-8334**		READE-190117/67
Freeimage Project					
Freeimage FreeImage is an input/output library written in C.					
Execute Code	06-01-2017	6.8	An exploitable out-of-bounds write vulnerability exists in the XMP image handling functionality of the FreeImage library. A specially crafted XMP file can cause an arbitrary memory overwrite resulting in code execution. An attacker can provide a malicious image to trigger this vulnerability. **Reference: CVE-2016-5684**	NA	A-FRE-FREEI-190117/68
Genixcms Project					
Genixcms GeniXCMS is a PHP Based Content Management System and Framework (CMSF).					
Execute Code; SQL Injection	01-01-2017	7.5	SQL injection vulnerability in register.php in GeniXCMS before 1.0.0 allows remote attackers to execute arbitrary SQL commands via the activation parameter. **Reference: CVE-2016-10096**	NA	A-GEN-GENIX-190117/69
Gstreamer					
Gstreamer GStreamer is a pipeline-based multimedia framework that links together a wide variety of media processing systems to complete complex workflows.					
Denial of Service	13-01-2017	4.3	The _parse_pat function in the mpegts parser in GStreamer before 1.10.2 allows remote attackers to cause a denial of service (NULL pointer dereference and crash) via a crafted file. **Reference: CVE-2016-9813**	https://gstreamer.freedesktop.org/releases/1.10/#1.10.2	A-GST-GSTRE-190117/70

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	13-01-2017	4.3	The gst_decode_chain_free_internal function in the flxdex decoder in gst-plugins-good in GStreamer before 1.10.2 allows remote attackers to cause a denial of service (invalid memory read and crash) via an invalid file, which triggers an incorrect unref call. **Reference: CVE-2016-9810**	https://gstreamer.freedesktop.org/releases/1.10/#1.10.2	A-GST-GSTRE-190117/71
NA	13-01-2017	6.8	Off-by-one error in the gst_h264_parse_set_caps function in GStreamer before 1.10.2 allows remote attackers to have unspecified impact via a crafted file, which triggers an out-of-bounds read. **Reference: CVE-2016-9809**	https://gstreamer.freedesktop.org/releases/1.10/#1.10.2	A-GST-GSTRE-190117/72
Denial of Service	13-01-2017	5	The FLIC decoder in GStreamer before 1.10.2 allows remote attackers to cause a denial of service (out-of-bounds write and crash) via a crafted series of skip and count pairs. **Reference: CVE-2016-9808**	https://gstreamer.freedesktop.org/releases/1.10/#1.10.2	A-GST-GSTRE-190117/73
Denial of Service	13-01-2017	4.3	The flx_decode_chunks function in gst/flx/gstflxdec.c in GStreamer before 1.10.2 allows remote attackers to cause a denial of service (invalid memory read and crash) via a crafted FLIC file. **Reference: CVE-2016-9807**	https://gstreamer.freedesktop.org/releases/1.10/#1.10.2	A-GST-GSTRE-190117/74
Hancom					
Hancom Office 2014 Hancom Office 2014 is the best mobile office application suite optimized for your printer.					
Execute Code; Overflow	06-01-2017	6.8	When opening a Hangul HShow Document (.hpt) and processing a structure within the document, Hancom Office 2014 will attempt to allocate space for a list of elements using a length from the file. When calculating this length,	NA	A-HAN-HANCO-190117/75

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

			an integer overflow can be made to occur which will cause the buffer to be undersized when the application tries to copy file data into the object containing this structure. This allows one to overwrite contiguous data in the heap which can lead to code-execution under the context of the application. **Reference: CVE-2016-4298**		
Execute Code; Overflow	06-01-2017	6.8	When opening a Hangul Hcell Document (.cell) and processing a record that uses the CSSValFormat object, Hancom Office 2014 will search for an underscore ("_") character at the end of the string and write a null terminator after it. If the character is at the very end of the string, the application will mistakenly write the null-byte outside the bounds of its destination. This can result in heap corruption that can lead code execution under the context of the application **Reference: CVE-2016-4296**	NA	A-HAN-HANCO-190117/76
Execute Code; Overflow	06-01-2017	6.8	When opening a Hangul Hcell Document (.cell) and processing a particular record within the Workbook stream, an index miscalculation leading to a heap overlow can be made to occur in Hancom Office 2014. The vulnerability occurs when processing data for a formula used to render a chart via the HncChartPlugin.hplg library. Due to a lack of bounds-checking when incrementing an index that is used for writing into a buffer for formulae, the application can be made to write pointer data outside its bounds	NA	A-HAN-HANCO-190117/77

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

			which can lead to code execution under the context of the application. **Reference: CVE-2016-4295**		
Execute Code; Overflow	06-01-2017	6.8	When opening a Hangul Hcell Document (.cell) and processing a property record within the Workbook stream, Hancom Office 2014 will attempt to allocate space for an element using a length from the file. When copying user-supplied data to this buffer, however, the application will use a different size which leads to a heap-based buffer overflow. This vulnerability can lead to code-execution under the context of the application. **Reference: CVE-2016-4294**	NA	A-HAN-HANCO-190117/78
Execute Code; Overflow	06-01-2017	6.8	When opening a Hangul HShow Document (.hpt) and processing a structure within the document, Hancom Office 2014 will use a static size to allocate a heap buffer yet explicitly trust a size from the file when modifying data inside of it. Due to this, an aggressor can corrupt memory outside the bounds of this buffer which can lead to code execution under the context of the application. **Reference: CVE-2016-4292**	NA	A-HAN-HANCO-190117/79
Execute Code; Overflow	06-01-2017	6.8	When opening a Hangul HShow Document (.hpt) and processing a structure within the document, Hancom Office 2014 will use a field from the structure in an operation that can cause the integer to overflow. This result is then used to allocate memory to copy file data in. Due to the lack of bounds checking on the integer, the allocated memory	NA	A-HAN-HANCO-190117/80

			buffer can be made to be undersized at which point the reading of file data will write outside the bounds of the buffer. This can lead to code execution under the context of the application. **Reference: CVE-2016-4291**		
Execute Code; Overflow	06-01-2017	6.8	When opening a Hangul HShow Document (.hpt) and processing a structure within the document, Hancom Office 2014 will attempt to allocate space for a block of data within the file. When calculating this length, the application will use a value from the file and add a constant to it without checking whether the addition of the constant will cause the integer to overflow which will cause the buffer to be undersized when the application tries to copy file data into it. This allows one to overwrite contiguous data in the heap which can lead to code-execution under the context of the application. **Reference: CVE-2016-4290**	NA	A-HAN-HANCO-190117/81
IBM; Pivotal Software					
Websphere Application Server/ Spring Security WebSphere Application Server (WAS) is a software product that performs the role of a web application server/ Spring Security is a Java/Java EE framework that provides authentication, authorization and other security features for enterprise applications.					
Bypass	06-01-2017	5	An issue was discovered in Pivotal Spring Security before 3.2.10, 4.1.x before 4.1.4, and 4.2.x before 4.2.1. Spring Security does not consider URL path parameters when processing security constraints. By adding a URL path parameter with an encoded "/" to a request, an attacker may be able to bypass a security constraint. The	https://pivotal.io/security/cve-2016-9879	A-IBM-WEBSP-190117/82

			root cause of this issue is a lack of clarity regarding the handling of path parameters in the Servlet Specification. Some Servlet containers include path parameters in the value returned for getPathInfo() and some do not. Spring Security uses the value returned by getPathInfo() as part of the process of mapping requests to security constraints. The unexpected presence of path parameters can cause a constraint to be bypassed. Users of Apache Tomcat (all current versions) are not affected by this vulnerability since Tomcat follows the guidance previously provided by the Servlet Expert group and strips path parameters from the value returned by getContextPath(), getServletPath(), and getPathInfo(). Users of other Servlet containers based on Apache Tomcat may or may not be affected depending on whether or not the handling of path parameters has been modified. Users of IBM WebSphere Application Server 8.5.x are known to be affected. Users of other containers that implement the Servlet specification may be affected. **Reference: CVE-2016-9879**		
ICU Project					
International Components For Unicode The International Components for Unicode (ICU) is a mature, portable set of C/C++ and Java libraries for software internationalization (I18N) and globalization (G11N) which implement the Unicode Standard, giving applications the same results on all platforms.					
Denial of Service; Overflow	04-01-2017	7.5	Stack-based buffer overflow in the ures_getByKeyWithFallback function in	https://bugzilla.redhat.com/show_	A-ICU-INTER-190117/83

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

			common/uresbund.cpp in International Components for Unicode (ICU) before 54.1 for C/C++ allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted uloc_getDisplayName call. **Reference: CVE-2014-9911**	bug.cgi?id=1383569	
ISC					
Bind BIND is open source software that enables you to publish your Domain Name System (DNS) information on the Internet, and to resolve DNS queries for your users.					
Denial of Service	12-01-2017	5	named in ISC BIND 9.x before 9.9.9-P5, 9.10.x before 9.10.4-P5, and 9.11.x before 9.11.0-P2 allows remote attackers to cause a denial of service (assertion failure and daemon exit) via a crafted DS resource record in an answer. **Reference: CVE-2016-9444**	https://kb.isc.org/article/AA-01441/74/CVE-2016-9444	A-ISC-BIND-190117/84
Denial of Service	12-01-2017	5	named in ISC BIND 9.9.9-P4, 9.9.9-S6, 9.10.4-P4, and 9.11.0-P1 allows remote attackers to cause a denial of service (assertion failure and daemon exit) via a response containing an inconsistency among the DNSSEC-related RRsets. **Reference: CVE-2016-9147**	https://kb.isc.org/article/AA-01440/74/CVE-2016-9147	A-ISC-BIND-190117/85
Denial of Service	12-01-2017	5	named in ISC BIND 9.x before 9.9.9-P5, 9.10.x before 9.10.4-P5, and 9.11.x before 9.11.0-P2 allows remote attackers to cause a denial of service (assertion failure and daemon exit) via a malformed response to an RTYPE ANY query. **Reference: CVE-2016-9131**	https://kb.isc.org/article/AA-01439/74/CVE-2016-9131	A-ISC-BIND-190117/86
Kaspersky					
Anti-virus; Internet Security; Total Security Kaspersky is a developer of anti-virus, anti-spyware, anti-spam and personal firewall products; Kaspersky Internet Security is an all-in-one security suite with improved design, faster scan times, and					

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

protection for online activity; Kaspersky Total Security helps you do more to ensure all your devices are protected so you can surf, shop & socialize more safely.					
Denial of Service; Bypass	06-01-2017	2.1	A local denial of service vulnerability exists in window broadcast message handling functionality of Kaspersky Anti-Virus software. Sending certain unhandled window messages, an attacker can cause application termination and in the same way bypass KAV self-protection mechanism. **Reference: CVE-2016-4329**	NA	A-KAS-ANTI--190117/87
Denial of Service	06-01-2017	2.1	A denial of service vulnerability exists in the IOCTL handling functionality of Kaspersky Internet Security KL1 driver. A specially crafted IOCTL signal can cause an access violation in KL1 kernel driver resulting in local system denial of service. An attacker can run a program from user-mode to trigger this vulnerability. **Reference: CVE-2016-4307**	NA	A-KAS-INTER-190117/88
Denial of Service	06-01-2017	2.1	A denial of service vulnerability exists in the syscall filtering functionality of Kaspersky Internet Security KLIF driver. A specially crafted native api call can cause a access violation in KLIF kernel driver resulting in local denial of service. An attacker can run program from user-mode to trigger this vulnerability. **Reference: CVE-2016-4305**	NA	A-KAS-INTER-190117/89
Denial of Service	06-01-2017	2.1	A denial of service vulnerability exists in the syscall filtering functionality of the Kaspersky Internet Security KLIF driver. A specially crafted native api call request can cause a access violation exception in KLIF kernel driver resulting in local	NA	A-KAS-INTER-190117/90

			denial of service. An attacker can run program from user-mode to trigger this vulnerability. **Reference: CVE-2016-4304**		
Bypass; Gain Information	06-01-2017	2.1	Multiple information leaks exist in various IOCTL handlers of the Kaspersky Internet Security KLDISK driver. Specially crafted IOCTL requests can cause the driver to return out-of-bounds kernel memory, potentially leaking sensitive information such as privileged tokens or kernel memory addresses that may be useful in bypassing kernel mitigations. An unprivileged user can run a program from user-mode to trigger this vulnerability. **Reference: CVE-2016-4306**	NA	A-KAS-TOTAL-190117/91
Lexmark					
Perceptive Document Filters Perceptive Document Filters is a single software development kit (SDK) that empowers software developers to perform deep inspection, format conversion, output manipulation and viewing for virtually any type of content.					
Execute Code; Overflow	06-01-2017	6.8	Exploitable heap overflow vulnerability exists in the Compound Binary File Format (CBFF) parser functionality of Lexmark Perceptive Document Filters library. A specially crafted CBFF file can cause a code execution. An attacker can send a malformed file to trigger this vulnerability. **Reference: CVE-2016-5646**	http://www.talosintelligence.com/reports/TALOS-2016-0185/	A-LEX-PERCE-190117/92
Execute Code; Overflow	06-01-2017	7.5	An exploitable out-of-bounds write exists in the Bzip2 parsing of the Lexmark Perspective Document Filters conversion functionality. A crafted Bzip2 document can lead to a stack-based buffer overflow causing an out-of-bounds write which	http://www.talosintelligence.com/reports/TALOS-2016-0173/	A-LEX-PERCE-190117/93

			under the right circumstance could potentially be leveraged by an attacker to gain arbitrary code execution. **Reference: CVE-2016-4336**		
Execute Code; Overflow	06-01-2017	6.8	An exploitable buffer overflow exists in the XLS parsing of the Lexmark Perspective Document Filters conversion functionality. A crafted XLS document can lead to a stack based buffer overflow resulting in remote code execution. **Reference: CVE-2016-4335**	NA	A-LEX-PERCE-190117/94
Libgd					
Libgd GD is an open source code library, written in C, for the dynamic creation of images by programmers.					
Denial of Service; Overflow	04-01-2017	5	Stack consumption vulnerability in the gdImageFillToBorder function in gd.c in the GD Graphics Library (aka libgd) before 2.2.2, as used in PHP before 5.6.28 and 7.x before 7.0.13, allows remote attackers to cause a denial of service (segmentation violation) via a crafted imagefilltoborder call that triggers use of a negative color value. **Reference: CVE-2016-9933**	https://github.com/php/php-src/commit/863d37ea66d5c960db08d6f4a2cbd2518f0f80d1	A-LIB-LIBGD-190117/95
Libimobiledevice					
Libplist libplist is a library to handle Apple Property List format whereas it's binary or XML.					
Denial of Service; Overflow; Gain Information	11-01-2017	6.4	The base64decode function in base64.c in libimobiledevice libplist through 1.12 allows attackers to obtain sensitive information from process memory or cause a denial of service (buffer over-read) via split encoded Apple Property List data. **Reference: CVE-2017-5209**	https://github.com/libimobiledevice/libplist/commit/3a55ddd3c4c11ce75a86afbefd085d8d397ff957	A-LIB-LIBPL-190117/96

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

Libtiff					
Libtiff Libtiff is a library for reading and writing Tagged Image File Format (abbreviated TIFF) files.					
Execute Code; Overflow	06-01-2017	6.8	An exploitable heap-based buffer overflow exists in the handling of TIFF images in LibTIFF's TIFF2PDF tool. A crafted TIFF document can lead to a heap-based buffer overflow resulting in remote code execution. Vulnerability can be triggered via a saved TIFF file delivered by other means. **Reference: CVE-2016-5652**	NA	A-LIB-LIBTI-190117/97
Execute Code; Overflow	12-01-2017	7.5	LibTIFF version 4.0.7 is vulnerable to a heap buffer overflow in the tools/tiffcp resulting in DoS or code execution via a crafted BitsPerSample value. **Reference: CVE-2017-5225**	http://bugzilla.maptools.org/show_bug.cgi?id=2656	A-LIB-LIBTI-190117/98
Liferay					
Liferay Portal Liferay Portal is a free and open source enterprise portal software product.					
Execute Code	13-01-2017	6.5	Liferay Portal through 6.2.10 allows remote authenticated users to execute arbitrary shell commands via a crafted Velocity template. **Reference: CVE-2010-5327**	https://issues.liferay.com/browse/LPS-7087	A-LIF-LIFER-190117/99
Linuxcontainers					
LXC LXC (Linux Containers) is an operating-system-level virtualization method for running multiple isolated Linux systems (containers) on a control host using a single Linux kernel.					
NA	09-01-2017	5	An issue was discovered in Linux Containers (LXC) before 2016-02-22. When executing a program via lxc-attach, the nonpriv session can escape to the parent session by using the TIOCSTI ioctl to push characters into the terminal's input buffer, allowing an attacker to escape the container.	https://github.com/lxc/lxc/commit/e986ea3dfa4a2957f71ae9bfaed406dd6e1ffff6	A-LIN-LXC-190117/100

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-2016-10124		
Mantisbt					
Mantisbt MantisBT is a popular free web-based bug tracking system.					
Cross Site Scripting	10-01-2017	4.3	Cross-site scripting (XSS) vulnerability in MantisBT Filter API in MantisBT versions before 1.2.19, and versions 2.0.0-beta1, 1.3.0-beta1 allows remote attackers to inject arbitrary web script or HTML via the 'view_type' parameter. **Reference: CVE-2016-6837**	https://mantisbt.org/bugs/view.php?id=21611	A-MAN-MANTI-190117/101
Matrixssl					
Matrixssl MatrixSSL is an Open-Source TLS/SSL implementation designed for custom applications in embedded hardware environments.					
Denial of Service; Cross Site Scripting	05-01-2017	5	The x509FreeExtensions function in MatrixSSL before 3.8.6 allows remote attackers to cause a denial of service (free of unallocated memory) via a crafted X.509 certificate. **Reference: CVE-2016-6892**	https://github.com/matrixssl/matrixssl/blob/3-8-6-open/CHANGES.md	A-MAT-MATRI-190117/102
Denial of Service; Cross Site Scripting	05-01-2017	5	MatrixSSL before 3.8.6 allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted ASN.1 Bit Field primitive in an X.509 certificate. **Reference: CVE-2016-6891**	https://github.com/matrixssl/matrixssl/blob/3-8-6-open/CHANGES.md	A-MAT-MATRI-190117/103
Execute Code; Overflow; Cross Site Scripting	05-01-2017	10	Heap-based buffer overflow in MatrixSSL before 3.8.6 allows remote attackers to execute arbitrary code via a crafted Subject Alt Name in an X.509 certificate. **Reference: CVE-2016-6890**	https://github.com/matrixssl/matrixssl/blob/3-8-6-open/CHANGES.md	A-MAT-MATRI-190117/104
Cross Site Scripting; Gain Information	13-01-2017	4.3	The pstm_exptmod function in MatrixSSL 3.8.6 and earlier does not properly perform modular expontiation, which might allow remote attackers to predict the secret key via a CRT attack.	http://www.matrixssl.org/blog/releases/matrixssl_3_8_4	A-MAT-MATRI-190117/105

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-2016-6887		
Denial of Service; Cross Site Scripting	13-01-2017	5	The pstm_reverse function in MatrixSSL before 3.8.4 allows remote attackers to cause a denial of service (invalid memory read and crash) via a (1) zero value or (2) the key's modulus for the secret key during RSA key exchange. **Reference: CVE-2016-6886**	http://www.matrixssl.org/blog/releases/matrixssl_3_8_4	A-MAT-MATRI-190117/106
Denial of Service; Cross Site Scripting	13-01-2017	5	The pstm_exptmod function in MatrixSSL before 3.8.4 allows remote attackers to cause a denial of service (invalid free and crash) via a base zero value for the modular exponentiation. **Reference: CVE-2016-6885**	http://www.matrixssl.org/blog/releases/matrixssl_3_8_4	A-MAT-MATRI-190117/107
Matroska					
Libebml libebml stands for Extensible Binary Meta Language library.					
NA	06-01-2017	5	A use-after-free / double-free vulnerability can occur in libebml master branch while parsing Track elements of the MKV container. **Reference: CVE-2016-1515**	NA	A-MAT-LIBEB-190117/108
Gain Information	06-01-2017	5	A specially crafted unicode string in libebml master branch can cause an off-by-few read on the heap in unicode string parsing code in libebml. This issue can potentially be used for information leaks. **Reference: CVE-2016-1514**	NA	A-MAT-LIBEB-190117/109
Mcafee					
Security Information And Event Management In the field of computer security, security information and event management (SIEM) software products and services combine security information management (SIM) and security event management (SEM).					
Bypass	05-01-2017	1.7	Authentication bypass vulnerability in Enterprise Security Manager (ESM) and License Manager (LM) in Intel Security McAfee Security	https://kc.mcafee.com/corporate/index?page=content&	A-MCA-SECUR-190117/110

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

			Information and Event Management (SIEM) 9.6.0 MR3 allows an administrator to make changes to other SIEM users' information including user passwords without supplying the current administrator password a second time via the GUI or GUI terminal commands. **Reference: CVE-2016-8006**	id=KB87744	
Metalgenix					
Genixcms GeniXCMS is a Free and Opensource CMS with a Simple and Fast website Load.					
Execute Code; SQL Injection	12-01-2017	6.5	SQL injection vulnerability in inc/mod/newsletter/options.php in GeniXCMS 0.0.8 allows remote authenticated administrators to execute arbitrary SQL commands via the recipient parameter to gxadmin/index.php. **Reference: CVE-2017-5347**	https://github.com/semplon/GeniXCMS/issues/61	A-MET-GENIX-190117/111
Execute Code; SQL Injection	12-01-2017	6.5	SQL injection vulnerability in inc/lib/Control/Backend/posts.control.php in GeniXCMS 0.0.8 allows remote authenticated administrators to execute arbitrary SQL commands via the id parameter to gxadmin/index.php. **Reference: CVE-2017-5346**	https://github.com/semplon/GeniXCMS/issues/61	A-MET-GENIX-190117/112
Execute Code; SQL Injection	12-01-2017	6.5	SQL injection vulnerability in inc/lib/Control/Ajax/tags-ajax.control.php in GeniXCMS 0.0.8 allows remote authenticated editors to execute arbitrary SQL commands via the term parameter to the default URI. **Reference: CVE-2017-5345**	NA	A-MET-GENIX-190117/113
Microsoft					
Edge Microsoft Edge is a web browser developed by Microsoft and included in Windows 10, Windows 10 Mobile, Xbox One, and Windows Holographic, replacing Internet Explorer as the default web browser					

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

on all device classes.					
Bypass	10-01-2017	6.8	Microsoft Edge allows remote attackers to bypass the Same Origin Policy via vectors involving the about:blank URL and data: URLs, aka "Microsoft Edge Elevation of Privilege Vulnerability." **Reference: CVE-2017-0002**	NA	A-MIC-EDGE-190117/114
Sharepoint Enterprise Server; Word SharePoint Server has been designed, developed, and tested with the Microsoft Software as a Service (SaaS) strategy at its core; Microsoft Word is a word processor developed by Microsoft.					
Execute Code; Overflow; Memory Corruption	10-01-2017	9.3	Microsoft Word 2016 and SharePoint Enterprise Server 2016 allow remote attackers to execute arbitrary code via a crafted document, aka "Microsoft Office Memory Corruption Vulnerability." **Reference: CVE-2017-0003**	NA	A-MIC-SHARE-190117/115
Netapp					
Clustered Data Ontap The Data ONTAP operating system implements a single proprietary file-system called WAFL.					
Gain Information	11-01-2017	4.3	Clustered Data ONTAP versions 8.0, 8.3.1, and 8.3.2 contain a default privileged account which under certain conditions can be used for unauthorized information disclosure. **Reference: CVE-2015-8020**	https://kb.netapp.com/support/s/article/cve-2015-8020-default-privileged-account-credentials-vulnerability-in-in-clustered-data-ontap?language=en_US	A-NET-CLUST-190117/116
Metrocluster Tiebreaker MetroCluster TieBreaker (MCTB) Solution is a plug-in that runs in the background as a Unix daemon on an OnCommand Unified Manager (OC UM) host.					
Gain	11-01-2017	5	MetroCluster Tiebreaker for	https://kb.	A-NET-

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

Information			clustered Data ONTAP in versions before 1.2 discloses sensitive information in cleartext which may be viewed by an unauthenticated user. **Reference: CVE-2016-6820**	netapp.com/support/s/article/cve-2016-6820-sensitive-information-disclosure-in-metrocluster-tiebreaker-for-clustered-data-ontap?language=en_US	METRO-190117/117
Netop					
Remote Control Netop Remote Control is a family of products that provides solutions for remote management, desktop sharing and support of various computer systems.					
Overflow	09-01-2017	4.3	Stack-based buffer overflow vulnerability in Netop Remote Control versions 11.53, 12.21 and prior. The affected module in the Guest client is the "Import to Phonebook" option. When a specially designed malicious file containing special characters is loaded, the overflow occurs. 12.51 is the fixed version. The Support case ref is 00109744. **Reference: CVE-2017-5216**	http://www.netop.com/fileadmin/netop/resources/products/administration/remote_control/release_notes/NetopRemoteControl_12.51_ModificationNotes_final.pdf	A-NET-REMOT-190117/118
Ntop					
Ntop ntop (stylized as ntop) is computer software that probes a computer network to show network use in a way similar to what the program top does for processes.					
Cross Site request	14-01-2017	6.8	Cross-site request forgery (CSRF) vulnerability in ntopng	https://github.com/nt	A-NTO-NTOP-

Forgery			through 2.4 allows remote attackers to hijack the authentication of arbitrary users, as demonstrated by admin/add_user.lua, admin/change_user_prefs.lua, admin/delete_user.lua, and admin/password_reset.lua. **Reference: CVE-2017-5473**	op/ntopng/commit/f91fbe3d94c8346884271838ae3406ae633f6f15	190117/119
NTP					
NTP Network Time Protocol (NTP) is a networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks.					
Gain Information	06-01-2017	5	An exploitable vulnerability exists in the message authentication functionality of libntp in ntp 4.2.8p4 and NTPSec a5fb34b9cc89b92a8fef2f459004865c93bb7f92. An attacker can send a series of crafted messages to attempt to recover the message digest key. **Reference: CVE-2016-1550**	http://www.oracle.com/technetwork/topics/security/linuxbulletinapr2016-2952096.html	A-NTP-NTP-190117/120
NA	06-01-2017	4	A malicious authenticated peer can create arbitrarily-many ephemeral associations in order to win the clock selection algorithm in ntpd in NTP 4.2.8p4 and earlier and NTPsec 3e160db8dc248a0bcb053b56a80167dc742d2b74 and a5fb34b9cc89b92a8fef2f459004865c93bb7f92 and modify a victim's clock. **Reference: CVE-2016-1549**	http://www.oracle.com/technetwork/topics/security/bulletinapr2016-2952098.html	A-NTP-NTP-190117/121
NA	06-01-2017	6.4	An attacker can spoof a packet from a legitimate ntpd server with an origin timestamp that matches the peer->dst timestamp recorded for that server. After making this switch, the client in NTP 4.2.8p4 and earlier and NTPSec aa48d001683e5b791a743ec9c5	http://www.oracle.com/technetwork/topics/security/linuxbulletinapr2016-2952096.html	A-NTP-NTP-190117/122

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

			75aaf7d867a2b0c will reject all future legitimate server responses. It is possible to force the victim client to move time after the mode has been changed. ntpq gives no indication that the mode has been switched. **Reference: CVE-2016-1548**		
NA	06-01-2017	5	An off-path attacker can cause a preemptible client association to be demobilized in NTP 4.2.8p4 and earlier and NTPSec a5fb34b9cc89b92a8fef2f459004865c93bb7f92 by sending a crypto NAK packet to a victim client with a spoofed source address of an existing associated peer. This is true even if authentication is enabled. **Reference: CVE-2016-1547**	http://www.oracle.com/technetwork/topics/security/bulletinapr2016-2952098.html	A-NTP-NTP-190117/123
Denial of Service	13-01-2017	5	ntpd in NTP before 4.2.8p9, when running on Windows, allows remote attackers to cause a denial of service via a large UDP packet. **Reference: CVE-2016-9312**	http://nwtime.org/ntp428p9_release/	A-NTP-NTP-190117/124
Denial of Service	13-01-2017	7.1	ntpd in NTP before 4.2.8p9, when the trap service is enabled, allows remote attackers to cause a denial of service (NULL pointer dereference and crash) via a crafted packet. **Reference: CVE-2016-9311**	http://nwtime.org/ntp428p9_release/	A-NTP-NTP-190117/125
NA	13-01-2017	6.4	The control mode (mode 6) functionality in ntpd in NTP before 4.2.8p9 allows remote attackers to set or unset traps via a crafted control mode packet. **Reference: CVE-2016-9310**	http://nwtime.org/ntp428p9_release/	A-NTP-NTP-190117/126
Denial of Service	13-01-2017	5	The read_mru_list function in NTP before 4.2.8p9 allows remote attackers to cause a denial of service (crash) via a	http://nwtime.org/ntp428p9_release/	A-NTP-NTP-190117/127

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

			crafted mrulist query. **Reference: CVE-2016-7434**		
NA	13-01-2017	5	NTP before 4.2.8p9 does not properly perform the initial sync calculations, which allows remote attackers to unspecified impact via unknown vectors, related to a "root distance that did not include the peer dispersion." **Reference: CVE-2016-7433**	http://nwtime.org/ntp428p9_release/	A-NTP-NTP-190117/128
Bypass	13-01-2017	5	NTP before 4.2.8p9 allows remote attackers to bypass the origin timestamp protection mechanism via an origin timestamp of zero. NOTE: this vulnerability exists because of a CVE-2015-8138 regression. **Reference: CVE-2016-7431**	http://nwtime.org/ntp428p9_release/	A-NTP-NTP-190117/129
Denial of Service	13-01-2017	4.3	NTP before 4.2.8p9 changes the peer structure to the interface it receives the response from a source, which allows remote attackers to cause a denial of service (prevent communication with a source) by sending a response for a source to an interface the source does not use. **Reference: CVE-2016-7429**	http://nwtime.org/ntp428p9_release/	A-NTP-NTP-190117/130
Denial of Service	13-01-2017	3.3	ntpd in NTP before 4.2.8p9 allows remote attackers to cause a denial of service (reject broadcast mode packets) via the poll interval in a broadcast packet. **Reference: CVE-2016-7428**	http://nwtime.org/ntp428p9_release/	A-NTP-NTP-190117/131
Denial of Service	13-01-2017	3.3	The broadcast mode replay prevention functionality in ntpd in NTP before 4.2.8p9 allows remote attackers to cause a denial of service (reject broadcast mode packets) via a crafted broadcast mode packet. **Reference: CVE-2016-7427**	http://nwtime.org/ntp428p9_release/	A-NTP-NTP-190117/132

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	13-01-2017	4.3	NTP before 4.2.8p9 rate limits responses received from the configured sources when rate limiting for all associations is enabled, which allows remote attackers to cause a denial of service (prevent responses from the sources) by sending responses with a spoofed source address. **Reference: CVE-2016-7426**	http://support.ntp.org/bin/view/Main/NtpBug3071	A-NTP-NTP-190117/133
Ntp-dev NTP-Dev is Debian Package Repository.					
Overflow	06-01-2017	5	An integer overflow can occur in NTP-dev.4.3.70 leading to an out-of-bounds memory copy operation when processing a specially crafted private mode packet. The crafted packet needs to have the correct message authentication code and a valid timestamp. When processed by the NTP daemon, it leads to an immediate crash. **Reference: CVE-2015-7848**	http://www.talosintelligence.com/reports/TALOS-2015-0052/	A-NTP-NTP-D-190117/134
Openbsd					
Openssh OpenSSH, also known as OpenBSD Secure Shell, [a] is a suite of security-related network-level utilities based on the SSH protocol, which help to secure network communications via the encryption of network traffic over multiple authentication methods and by providing secure tunneling capabilities.					
Overflow; Gain Privileges	04-01-2017	7.2	The shared memory manager (associated with pre-authentication compression) in sshd in OpenSSH before 7.4 does not ensure that a bounds check is enforced by all compilers, which might allows local users to gain privileges by leveraging access to a sandboxed privilege-separation process, related to the m_zback and m_zlib data structures. **Reference: CVE-2016-10012**	https://www.openssh.com/txt/release-7.4	A-OPE-OPENS-190117/135
Gain	04-01-2017	2.1	authfile.c in sshd in OpenSSH	https://git	A-OPE-

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

Information			before 7.4 does not properly consider the effects of realloc on buffer contents, which might allow local users to obtain sensitive private-key information by leveraging access to a privilege-separated child process. **Reference: CVE-2016-10011**	hub.com/openbsd/src/commit/ac8147a06ed2e2403fb6b9a0c03e618a9333c0e9	OPENS-190117/136
Gain Privileges	04-01-2017	6.9	sshd in OpenSSH before 7.4, when privilege separation is not used, creates forwarded Unix-domain sockets as root, which might allow local users to gain privileges via unspecified vectors, related to serverloop.c. **Reference: CVE-2016-10010**	https://github.com/openbsd/src/commit/c76fac666ea038753294f2ac94d310f8adece9ce	A-OPE-OPENS-190117/137
NA	04-01-2017	7.5	Untrusted search path vulnerability in ssh-agent.c in ssh-agent in OpenSSH before 7.4 allows remote attackers to execute arbitrary local PKCS#11 modules by leveraging control over a forwarded agent-socket. **Reference: CVE-2016-10009**	https://www.openssh.com/txt/release-7.4	A-OPE-OPENS-190117/138
PHP					
PHP PHP (recursive acronym for PHP: Hypertext Preprocessor) is a widely-used open source general-purpose scripting language that is especially suited for web development and can be embedded into HTML.					
Denial of Service	04-01-2017	7.5	The unserialize implementation in ext/standard/var.c in PHP 7.x before 7.0.14 allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via crafted serialized data. NOTE: this vulnerability exists because of an incomplete fix for CVE-2015-6834. **Reference: CVE-2016-9936**	https://github.com/php/php-src/commit/b2af4e8868726a040234de113436c6e4f6372d17	A-PHP-PHP-190117/139
Denial of Service;	04-01-2017	7.5	The php_wddx_push_element function in ext/wddx/wddx.c in	https://bugs.php.net/b	A-PHP-PHP-190117/140

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

Memory Corruption			PHP before 5.6.29 and 7.x before 7.0.14 allows remote attackers to cause a denial of service (out-of-bounds read and memory corruption) or possibly have unspecified other impact via an empty boolean element in a wddxPacket XML document. **Reference: CVE-2016-9935**	ug.php?id=73631	
Denial of Service	04-01-2017	5	ext/wddx/wddx.c in PHP before 5.6.28 and 7.x before 7.0.13 allows remote attackers to cause a denial of service (NULL pointer dereference) via crafted serialized data in a wddxPacket XML document, as demonstrated by a PDORow string. **Reference: CVE-2016-9934**	https://bugs.php.net/bug.php?id=73331	A-PHP-PHP-190117/141
Denial of Service	04-01-2017	7.5	PHP through 5.6.27 and 7.x through 7.0.12 mishandles property modification during __wakeup processing, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted serialized data, as demonstrated by Exception::__toString with DateInterval::__wakeup. **Reference: CVE-2016-9138**	https://bugs.php.net/bug.php?id=73147	A-PHP-PHP-190117/142
Denial of Service	04-01-2017	7.5	Use-after-free vulnerability in the CURLFile implementation in ext/curl/curl_file.c in PHP before 5.6.27 and 7.x before 7.0.12 allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted serialized data that is mishandled during __wakeup processing. **Reference: CVE-2016-9137**	https://bugs.php.net/bug.php?id=73147	A-PHP-PHP-190117/143
Denial of Service; Overflow	04-01-2017	7.5	The get_icu_disp_value_src_php function in ext/intl/locale/locale_methods.c in PHP before 5.3.29, 5.4.x	https://bugzilla.redhat.com/show_bug.cgi?id=	A-PHP-PHP-190117/144

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

			before 5.4.30, and 5.5.x before 5.5.14 does not properly restrict calls to the ICU uresbund.cpp component, which allows remote attackers to cause a denial of service (buffer overflow) or possibly have unspecified other impact via a locale_get_display_name call with a long first argument. **Reference: CVE-2014-9912**	1383569	
Denial of Service; Execute Code; Overflow	11-01-2017	7.5	Zend/zend_hash.c in PHP before 7.0.15 and 7.1.x before 7.1.1 mishandles certain cases that require large array allocations, which allows remote attackers to execute arbitrary code or cause a denial of service (integer overflow, uninitialized memory access, and use of arbitrary destructor function pointers) via crafted serialized data. **Reference: CVE-2017-5340**	https://bugs.php.net/bug.php?id=73832	A-PHP-PHP-190117/145
Denial of Service; Execute Code; Overflow	11-01-2017	7.5	The SplObjectStorage unserialize implementation in ext/spl/spl_observer.c in PHP before 7.0.12 does not verify that a key is an object, which allows remote attackers to execute arbitrary code or cause a denial of service (uninitialized memory access) via crafted serialized data. **Reference: CVE-2016-7480**	NA	A-PHP-PHP-190117/146
Execute Code	11-01-2017	7.5	In all versions of PHP 7, during the unserialization process, resizing the 'properties' hash table of a serialized object may lead to use-after-free. A remote attacker may exploit this bug to gain arbitrary code execution. **Reference: CVE-2016-7479**	NA	A-PHP-PHP-190117/147
Denial of Service	11-01-2017	5	Zend/zend_exceptions.c in PHP, possibly 5.x before 5.6.28 and 7.x before 7.0.13, allows remote	NA	A-PHP-PHP-190117/148

			attackers to cause a denial of service (infinite loop) via a crafted Exception object in serialized data, a related issue to CVE-2015-8876. **Reference: CVE-2016-7478**		
Pivotal Software					
Gemfire For Pivotal Cloud Foundry GemFire for Pivotal Cloud Foundry delivers one of the market's most powerful in memory technologies on Pivotal's open cloud native application platform.					
Denial of Service	06-01-2017	7.5	An issue was discovered in Pivotal GemFire for PCF 1.6.x versions prior to 1.6.5 and 1.7.x versions prior to 1.7.1. The gfsh (Geode Shell) endpoint, used by operators and application developers to connect to their cluster, is unauthenticated and publicly accessible. Because HTTPS communications are terminated at the gorouter, communications from the gorouter to GemFire clusters are unencrypted. An attacker could run any command available on gfsh and could cause denial of service, lost confidentiality of data, escalate privileges, or eavesdrop on other communications between the gorouter and the cluster. **Reference: CVE-2016-9885**	https://pivotal.io/security/cve-2016-9885	A-PIV-GEMFI-190117/149
Piwigo					
Piwigo Piwigo is photo gallery software for the web, built by an active community of users and developers.					
Execute Code	03-01-2017	7.5	admin/plugin.php in Piwigo through 2.8.3 doesn't validate the sections variable while using it to include files. This can cause information disclosure and code execution if it contains a .. sequence. **Reference: CVE-2016-10105**	https://github.com/Piwigo/Piwigo/issues/574#issuecomment-267938358	A-PIW-PIWIG-190117/150

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

Puppetlabs					
Puppet In computing, Puppet is an open-source configuration management tool.					
NA	12-01-2017	5.8	Open redirect vulnerability in the Console in Puppet Enterprise 2015.x and 2016.x before 2016.4.0 allows remote attackers to redirect users to arbitrary web sites and conduct phishing attacks via a // (slash slash) followed by a domain in the redirect parameter. NOTE: this vulnerability exists because of an incomplete fix for CVE-2015-6501. **Reference: CVE-2016-5715**	https://puppet.com/security/cve/cve-2016-5715	A-PUP-PUPPE-190117/151
NA	12-01-2017	5.8	Open redirect vulnerability in the Console in Puppet Enterprise before 2015.2.1 allows remote attackers to redirect users to arbitrary web sites and conduct phishing attacks via the string parameter. **Reference: CVE-2015-6501**	https://puppet.com/security/cve/CVE-2015-6501	A-PUP-PUPPE-190117/152
Python Software Foundation					
Hpack; Hyper The mission of the Python Software Foundation is to promote, protect, and advance the Python programming language, and to support and facilitate the growth of a diverse and international community of Python programmers.					
Denial of Service	10-01-2017	7.8	A HTTP/2 implementation built using any version of the Python HPACK library between v1.0.0 and v2.2.0 could be targeted for a denial of service attack, specifically a so-called "HPACK Bomb" attack. This attack occurs when an attacker inserts a header field that is exactly the size of the HPACK dynamic header table into the dynamic header table. The attacker can then send a header block that is simply repeated requests to expand that field in the dynamic	https://python-hyper.org/hpack/en/latest/security/CVE-2016-6581.html	A-PYT-HPACK-190117/153

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

			table. This can lead to a gigantic compression ratio of 4,096 or better, meaning that 16kB of data can decompress to 64MB of data on the target machine. **Reference: CVE-2016-6581**		
Python Priority Library The mission of the Python Software Foundation is to promote, protect, and advance the Python programming language, and to support and facilitate the growth of a diverse and international community of Python programmers.					
NA	10-01-2017	5	A HTTP/2 implementation built using any version of the Python priority library prior to version 1.2.0 could be targeted by a malicious peer by having that peer assign priority information for every possible HTTP/2 stream ID. The priority tree would happily continue to store the priority information for each stream, and would therefore allocate unbounded amounts of memory. Attempting to actually use a tree like this would also cause extremely high CPU usage to maintain the tree. **Reference: CVE-2016-6580**	https://python-hyper.org/priority/en/latest/security/CVE-2016-6580.html	A-PYT-PYTHO-190117/154
Quick Heal					
Antivirus Pro;Internet Security;Total Security Quick Heal offers a wide range of antivirus products for Home Users that protects your PC from viruses, spywares, malwares.					
Execute Code; Overflow	02-01-2017	7.5	Stack-based buffer overflow in Quick Heal Internet Security 10.1.0.316 and earlier, Total Security 10.1.0.316 and earlier, and AntiVirus Pro 10.1.0.316 and earlier on OS X allows remote attackers to execute arbitrary code via a crafted LC_UNIXTHREAD.cmdsize field in a Mach-O file that is mishandled during a Security Scan (aka Custom Scan) operation.	NA	A-QUI-ANTIV-190117/155

			Reference: CVE-2017-5005		
Ruby-lang					
Ruby Ruby is a dynamic, reflective, object-oriented, general-purpose programming language.					
Overflow	06-01-2017	7.5	An exploitable heap overflow vulnerability exists in the Fiddle::Function.new "initialize" function functionality of Ruby. In Fiddle::Function.new "initialize" heap buffer "arg_types" allocation is made based on args array length. Specially constructed object passed as element of args array can increase this array size after mentioned allocation and cause heap overflow. **Reference: CVE-2016-2339**	http://www.talosintelligence.com/reports/TALOS-2016-0034/	A-RUB-RUBY-190117/156
Execute Code	06-01-2017	7.5	Type confusion exists in _cancel_eval Ruby's TclTkIp class method. Attacker passing different type of object than String as "retval" argument can cause arbitrary code execution. **Reference: CVE-2016-2337**	http://www.talosintelligence.com/reports/TALOS-2016-0031/	A-RUB-RUBY-190117/157
Execute Code	06-01-2017	7.5	Type confusion exists in two methods of Ruby's WIN32OLE class, ole_invoke and ole_query_interface. Attacker passing different type of object than this assumed by developers can cause arbitrary code execution. **Reference: CVE-2016-2336**	http://www.talosintelligence.com/reports/TALOS-2016-0029/	A-RUB-RUBY-190117/158
S9Y					
Serendipity Serendipity is a PHP-powered weblog engine which gives the user an easy way to maintain a blog.					
Cross Site request Forgery	14-01-2017	6.8	Serendipity through 2.0.5 allows CSRF for the installation of an event plugin or a sidebar plugin. **Reference: CVE-2017-5476**	https://github.com/s9y/Serendipity/issues/439	A-S9Y-SEREN-190117/159
Cross Site request	14-01-2017	6.8	comment.php in Serendipity through 2.0.5 allows CSRF in	https://github.com/s	A-S9Y-SEREN-

Forgery			deleting any comments. **Reference: CVE-2017-5475**	9y/Serendipity/issues/439	190117/160
NA	14-01-2017	5.8	Open redirect vulnerability in comment.php in Serendipity through 2.0.5 allows remote attackers to redirect users to arbitrary web sites and conduct phishing attacks via a URL in the HTTP Referer header. **Reference: CVE-2017-5474**	https://github.com/s9y/Serendipity/commit/628593347 0bab2923e4573b5d54ba9a32629b0cd	A-S9Y-SEREN-190117/161
Schedmd					
Slurm Slurm is a Highly Scalable Workload Manager.					
NA	05-01-2017	7.6	The _prolog_error function in slurmd/req.c in Slurm before 15.08.13, 16.x before 16.05.7, and 17.x before 17.02.0-pre4 has a vulnerability in how the slurmd daemon informs users of a Prolog failure on a compute node. That vulnerability could allow a user to assume control of an arbitrary file on the system. Any exploitation of this is dependent on the user being able to cause or anticipate the failure (non-zero return code) of a Prolog script that their job would run on. This issue affects all Slurm versions from 0.6.0 (September 2005) to present. Workarounds to prevent exploitation of this are to either disable your Prolog script, or modify it such that it always returns 0 ("success") and adjust it to set the node as down using scontrol instead of relying on the slurmd to handle that automatically. If you do not have a Prolog set you are unaffected by this issue.	https://www.schedmd.com/news.php?id=178	A-SCH-SLURM-190117/162

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-2016-10030		
Splunk					
Splunk Splunk is an American multinational corporation based in San Francisco, California, that produces software for searching, monitoring, and analyzing machine-generated big data, via a web-style interface.					
Gain Information	10-01-2017	10	Splunk Web in Splunk Enterprise 5.0.x before 5.0.17, 6.0.x before 6.0.13, 6.1.x before 6.1.12, 6.2.x before 6.2.12, 6.3.x before 6.3.8, and 6.4.x before 6.4.4 allows remote attackers to conduct HTTP request injection attacks and obtain sensitive REST API authentication-token information via unspecified vectors, aka SPL-128840. **Reference: CVE-2016-10126**	https://www.splunk.com/view/SP-CAAAPSR	A-SPL-SPLUN-190117/163
Tenable					
Nessus Nessus is the most trusted vulnerability scanning platform for auditors and security analysts.					
Cross Site Scripting	05-01-2017	3.5	Cross-site scripting (XSS) vulnerability in Tenable Nessus before 6.9.3 allows remote authenticated users to inject arbitrary web script or HTML via unspecified vectors. **Reference: CVE-2017-5179**	https://www.tenable.com/security/tns-2017-01	A-TEN-NESSU-190117/164
Veritas					
Netbackup Appliance Firmware The NetBackup appliances are Veritas-defined platforms of hardware, firmware and software.					
Execute Code	04-01-2017	10	scripts/license.pl in Veritas NetBackup Appliance 2.6.0.x through 2.6.0.4, 2.6.1.x through 2.6.1.2, 2.7.x through 2.7.3, and 3.0.x allow remote attackers to execute arbitrary commands via shell metacharacters in the hostName parameter to appliancews/getLicense. **Reference: CVE-2016-7399**	https://www.veritas.com/support/en_US/article.000116055	A-VER-NETBA-190117/165

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

Web2py					
Web2py An open source full-stack python web framework for scalable, secure and portable web applications.					
Cross Site Scripting	11-01-2017	3.5	Web2py versions 2.14.5 and below was affected by Reflected XSS vulnerability, which allows an attacker to perform an XSS attack on logged in user (admin). **Reference: CVE-2016-4807**	NA	A-WEB-WEB2P-190117/166
Western Digital					
Mycloud Nas WD My Cloud is a personal cloud storage unit to organize your photos and videos.					
NA	03-01-2017	10	Unauthenticated Remote Command injection as root occurs in the Western Digital MyCloud NAS 2.11.142 /web/google_analytics.php URL via a modified arg parameter in the POST data. **Reference: CVE-2016-10108**	NA	A-WES-MYCLO-190117/167
NA	03-01-2017	10	Unauthenticated Remote Command injection as root occurs in the Western Digital MyCloud NAS 2.11.142 index.php page via a modified Cookie header. **Reference: CVE-2016-10107**	NA	A-WES-MYCLO-190117/168
Woocommerce					
Woocommerce WooCommerce is an open source e-commerce plugin for WordPress.					
Cross Site Scripting	03-01-2017	3.5	Cross-site scripting (XSS) vulnerability in the WooCommerce plugin before 2.6.9 for WordPress allows remote authenticated administrators to inject arbitrary web script or HTML by providing crafted tax-rate table values in CSV format. **Reference: CVE-2016-10112**	https://wordpress.org/plugins/woocommerce/changelog/	A-WOO-WOOCO-190117/169
Wordpress					
Wordpress WordPress is a free and open-source content management system (CMS) based on PHP and MySQL.					
Directory	04-01-2017	6.5	Directory traversal vulnerability	https://wo	A-WOR-

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

Traversal			in the File_Upload_Upgrader class in wp-admin/includes/class-file-upload-upgrader.php in the upgrade package uploader in WordPress before 4.6.1 allows remote authenticated users to access arbitrary files via a crafted urlholder parameter. **Reference: CVE-2016-7169**	rdpress.org/news/2016/09/wordpress-4-6-1-security-and-maintenance-release/	WORDP-190117/170
Cross Site Scripting	04-01-2017	3.5	Cross-site scripting (XSS) vulnerability in the media_handle_upload function in wp-admin/includes/media.php in WordPress before 4.6.1 might allow remote attackers to inject arbitrary web script or HTML by tricking an administrator into uploading an image file that has a crafted filename. **Reference: CVE-2016-7168**	https://wordpress.org/news/2016/09/wordpress-4-6-1-security-and-maintenance-release/	A-WOR-WORDP-190117/171
Bypass	14-01-2017	5	wp-includes/ms-functions.php in the Multisite WordPress API in WordPress before 4.7.1 does not properly choose random numbers for keys, which makes it easier for remote attackers to bypass intended access restrictions via a crafted (1) site signup or (2) user signup. **Reference: CVE-2017-5493**	https://codex.wordpress.org/Version_4.7.1	A-WOR-WORDP-190117/172
Cross Site request Forgery	14-01-2017	6.8	Cross-site request forgery (CSRF) vulnerability in the widget-editing accessibility-mode feature in WordPress before 4.7.1 allows remote attackers to hijack the authentication of unspecified victims for requests that perform a widgets-access action, related to wp-admin/includes/class-wp-screen.php and wp-admin/widgets.php. **Reference: CVE-2017-5492**	https://codex.wordpress.org/Version_4.7.1	A-WOR-WORDP-190117/173

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

Bypass	14-01-2017	5	wp-mail.php in WordPress before 4.7.1 might allow remote attackers to bypass intended posting restrictions via a spoofed mail server with the mail.example.com name. **Reference: CVE-2017-5491**	https://codex.wordpress.org/Version_4.7.1	A-WOR-WORDP-190117/174
Cross Site Scripting	14-01-2017	4.3	Cross-site scripting (XSS) vulnerability in the theme-name fallback functionality in wp-includes/class-wp-theme.php in WordPress before 4.7.1 allows remote attackers to inject arbitrary web script or HTML via a crafted directory name of a theme, related to wp-admin/includes/class-theme-installer-skin.php. **Reference: CVE-2017-5490**	https://wordpress.org/news/2017/01/wordpress-4-7-1-security-and-maintenance-release/	A-WOR-WORDP-190117/175
Cross Site request Forgery	14-01-2017	6.8	Cross-site request forgery (CSRF) vulnerability in WordPress before 4.7.1 allows remote attackers to hijack the authentication of unspecified victims via vectors involving a Flash file upload. **Reference: CVE-2017-5489**	https://codex.wordpress.org/Version_4.7.1	A-WOR-WORDP-190117/176
Cross Site Scripting	14-01-2017	4.3	Multiple cross-site scripting (XSS) vulnerabilities in wp-admin/update-core.php in WordPress before 4.7.1 allow remote attackers to inject arbitrary web script or HTML via the (1) name or (2) version header of a plugin. **Reference: CVE-2017-5488**	https://codex.wordpress.org/Version_4.7.1	A-WOR-WORDP-190117/177
Gain Information	14-01-2017	5	wp-includes/rest-api/endpoints/class-wp-rest-users-controller.php in the REST API implementation in WordPress 4.7 before 4.7.1 does not properly restrict listings of post authors, which allows remote attackers to obtain sensitive information via a wp-	https://wordpress.org/news/2017/01/wordpress-4-7-1-security-and-maintenance-release/	A-WOR-WORDP-190117/178

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

			json/wp/v2/users request. **Reference: CVE-2017-5487**		
Zoneminder					
Zoneminder ZoneMinder is a free, open source Closed-circuit television software application developed for Linux which supports IP, USB and Analog cameras.					
Bypass; Gain Information	13-01-2017	5	Information disclosure and authentication bypass vulnerability exists in the Apache HTTP Server configuration bundled with ZoneMinder v1.30.0, which allows a remote unauthenticated attacker to browse all directories in the web root, e.g., a remote unauthenticated attacker can view all CCTV images on the server. **Reference: CVE-2016-10140**	https://github.com/ZoneMinder/ZoneMinder/pull/1697	A-ZON-ZONEM-190117/179
Application; Operating System (A/OS)					
Canonical; Debian/Pidgin					
Ubuntu Linux/Debian Linux/Pidgin Ubuntu is a Debian-based Linux operating system for personal computers, tablets and smart-phones/ Debian is an operating system and a distribution of Free Software/ Pidgin is a chat program which lets you log in to accounts on multiple chat networks simultaneously.					
Directory Traversal	06-01-2017	5.8	A directory traversal exists in the handling of the MXIT protocol in Pidgin. Specially crafted MXIT data sent from the server could potentially result in overwrite of files. A malicious server or someone with access to the network traffic can provide an invalid filename for a splash image triggering the vulnerability. **Reference: CVE-2016-4323**	http://www.pidgin.im/news/security/?id=97	A-OS-CAN-UBUNT-190117/180
Gain Information	06-01-2017	4.3	An information leak exists in the handling of the MXIT protocol in Pidgin. Specially crafted MXIT data sent to the server could potentially result in an out-of-bounds read. A user could be convinced to enter a particular	http://www.pidgin.im/news/security/?id=96	A-OS-CAN-UBUNT-190117/181

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

			string which would then get converted incorrectly and could lead to a potential out-of-bounds read. **Reference: CVE-2016-2380**		
Overflow; Memory Corruption	06-01-2017	6.8	Buffer overflow vulnerability exists in the handling of the MXIT protocol Pidgin. Specially crafted data sent via the server could potentially result in a buffer overflow, potentially resulting in memory corruption. A malicious server or an unfiltered malicious user can send negative length values to trigger this vulnerability. **Reference: CVE-2016-2378**	http://www.pidgin.im/news/security/?id=94	A-OS-CAN-UBUNT-190117/182
Overflow	06-01-2017	6.8	Buffer overflow vulnerability exists in the handling of the MXIT protocol in Pidgin. Specially crafted MXIT data sent by the server could potentially result in an out-of-bounds write of one byte. A malicious server can send a negative content-length in response to a HTTP request triggering the vulnerability. **Reference: CVE-2016-2377**	http://www.pidgin.im/news/security/?id=93	A-OS-CAN-UBUNT-190117/183
Execute Code; Overflow	06-01-2017	6.8	Buffer overflow vulnerability exists in the handling of the MXIT protocol in Pidgin. Specially crafted MXIT data sent from the server could potentially result in arbitrary code execution. A malicious server or an attacker who intercepts the network traffic can send an invalid size for a packet which will trigger a buffer overflow. **Reference: CVE-2016-2376**	http://www.pidgin.im/news/security/?id=92	A-OS-CAN-UBUNT-190117/184
NA	06-01-2017	5	An exploitable out-of-bounds read exists in the handling of the MXIT protocol in Pidgin. Specially crafted MXIT contact	http://www.pidgin.im/news/security/?id=1	A-OS-CAN-UBUNT-190117/185

			information sent from the server can result in memory disclosure. **Reference: CVE-2016-2375**	08	
Execute Code; Memory Corruption	06-01-2017	6.8	An exploitable memory corruption vulnerability exists in the handling of the MXIT protocol in Pidgin. Specially crafted MXIT MultiMX message sent via the server can result in an out-of-bounds write leading to memory disclosure and code execution. **Reference: CVE-2016-2374**	http://www.pidgin.im/news/security/?id=107	A-OS-CAN-UBUNT-190117/186
Denial of Service	06-01-2017	4.3	A denial of service vulnerability exists in the handling of the MXIT protocol in Pidgin. Specially crafted MXIT data sent via the server could potentially result in an out-of-bounds read. A malicious server or user can send an invalid mood to trigger this vulnerability. **Reference: CVE-2016-2373**	http://www.pidgin.im/news/security/?id=106	A-OS-CAN-UBUNT-190117/187
Denial of Service; Gain Information	06-01-2017	4.9	An information leak exists in the handling of the MXIT protocol in Pidgin. Specially crafted MXIT data sent via the server could potentially result in an out-of-bounds read. A malicious user, server, or man-in-the-middle attacker can send an invalid size for a file transfer which will trigger an out-of-bounds read vulnerability. This could result in a denial of service or copy data from memory to the file, resulting in an information leak if the file is sent to another user. **Reference: CVE-2016-2372**	http://www.pidgin.im/news/security/?id=105	A-OS-CAN-UBUNT-190117/188
Execute Code; Memory Corruption	06-01-2017	6.8	An out-of-bounds write vulnerability exists in the handling of the MXIT protocol in Pidgin. Specially crafted MXIT data sent via the server could cause memory corruption	http://www.pidgin.im/news/security/?id=104	A-OS-CAN-UBUNT-190117/189

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

			resulting in code execution. **Reference: CVE-2016-2371**		
Denial of Service	06-01-2017	4.3	A denial of service vulnerability exists in the handling of the MXIT protocol in Pidgin. Specially crafted MXIT data sent from the server could potentially result in an out-of-bounds read. A malicious server or man-in-the-middle attacker can send invalid data to trigger this vulnerability. **Reference: CVE-2016-2370**	http://www.pidgin.im/news/security/?id=103	A-OS-CAN-UBUNT-190117/190
Denial of Service	06-01-2017	4.3	A NULL pointer dereference vulnerability exists in the handling of the MXIT protocol in Pidgin. Specially crafted MXIT data sent via the server could potentially result in a denial of service vulnerability. A malicious server can send a packet starting with a NULL byte triggering the vulnerability. **Reference: CVE-2016-2369**	http://www.pidgin.im/news/security/?id=102	A-OS-CAN-UBUNT-190117/191
Execute Code; Overflow; Memory Corruption	06-01-2017	7.5	Multiple memory corruption vulnerabilities exist in the handling of the MXIT protocol in Pidgin. Specially crafted MXIT data sent via the server could result in multiple buffer overflows, potentially resulting in code execution or memory disclosure. **Reference: CVE-2016-2368**	http://www.pidgin.im/news/security/?id=101	A-OS-CAN-UBUNT-190117/192
Denial of Service; Gain Information	06-01-2017	3.5	An information leak exists in the handling of the MXIT protocol in Pidgin. Specially crafted MXIT data sent via the server could potentially result in an out-of-bounds read. A malicious user, server, or man-in-the-middle can send an invalid size for an avatar which will trigger an out-of-bounds read vulnerability. This could result in a denial of	http://www.pidgin.im/news/security/?id=100	A-OS-CAN-UBUNT-190117/193

			service or copy data from memory to the file, resulting in an information leak if the avatar is sent to another user. **Reference: CVE-2016-2367**		
Denial of Service	06-01-2017	4.3	A denial of service vulnerability exists in the handling of the MXIT protocol in Pidgin. Specially crafted MXIT data sent via the server could potentially result in an out-of-bounds read. A malicious server or an attacker who intercepts the network traffic can send invalid data to trigger this vulnerability and cause a crash. **Reference: CVE-2016-2366**	http://www.pidgin.im/news/security/?id=99	A-OS-CAN-UBUNT-190117/194
Denial of Service	06-01-2017	4.3	A denial of service vulnerability exists in the handling of the MXIT protocol in Pidgin. Specially crafted MXIT data sent via the server could potentially result in a null pointer dereference. A malicious server or an attacker who intercepts the network traffic can send invalid data to trigger this vulnerability and cause a crash. **Reference: CVE-2016-2365**	http://www.pidgin.im/news/security/?id=98	A-OS-CAN-UBUNT-190117/195
Fedoraproject/Libbsd					
Fedora/Libbsd Fedora (formerly Fedora Core) is an operating system based on the Linux kernel, developed by the community-supported Fedora Project and sponsored by Red Hat/ Libbsd provides useful functions commonly found on BSD systems, and lacking on others like GNU systems, thus making it easier to port projects with strong BSD origins, without needing to embed the same code over and over again on each project.					
Overflow	13-01-2017	7.5	Off-by-one vulnerability in the fgetwln function in libbsd before 0.8.2 allows attackers to have unspecified impact via unknown vectors, which trigger a heap-based buffer overflow. **Reference: CVE-2016-2090**	https://cgit.freedesktop.org/libbsd/commit/?id=c8f0723d2b4520bdd6b9eb7c3e7976de7	A-OS-FED-FEDOR-190117/196

				26d7ff7	
Operating System (OS)					
Arista					
Dcs-7050q Eos Software;Dcs-7050s Eos Software;Dcs-7050t Eos Software NA					
Denial of Service	04-01-2017	7.8	Arista EOS 4.15 before 4.15.8M, 4.16 before 4.16.7M, and 4.17 before 4.17.0F on DCS-7050 series devices allow remote attackers to cause a denial of service (device reboot) by sending crafted packets to the control plane. **Reference: CVE-2016-6894**	https://www.arista.com/en/support/advisories-notices/security-advisories/1752-security-advisory-25	O-ARI-DCS-7-190117/197
Barco					
Clickshare Csc-1 Firmware;Clickshare Cse-200 Firmware NA					
Cross Site Scripting	12-01-2017	4.3	Cross-site scripting (XSS) vulnerability in wallpaper.php in the Base Unit in Barco ClickShare CSC-1 devices with firmware before 01.09.03, CSM-1 devices with firmware before 01.06.02, and CSE-200 devices with firmware before 01.03.02 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors. **Reference: CVE-2016-3150**	NA	O-BAR-CLICK-190117/198
D-link					
Dgs-1100 Firmware NA					
NA	09-01-2017	6.8	D-Link DGS-1100 devices with Rev.B firmware 1.01.018 have a hardcoded SSL private key, which allows man-in-the-middle attackers to spoof devices by hijacking an HTTPS session. **Reference: CVE-2016-10125**	NA	O-D-L-DGS-1-190117/199

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

Genexia					
Drgos NA					
Execute Code	05-01-2017	9	The Parental Control panel in Genexis devices with DRGOS before 1.14.1 allows remote authenticated users to execute arbitrary CLI commands via the (1) start_hour, (2) start_minute, (3) end_hour, (4) end_minute, or (5) hostname parameter. **Reference: CVE-2015-3441**	https://www.navixia.com/CVE-2015-3441.txt	O-GEN-DRGOS-190117/200
Google					
Android Android is a mobile operating system developed by Google, based on the Linux kernel and designed primarily for touchscreen mobile devices.					
Execute Code	12-01-2017	7.6	An elevation of privilege vulnerability in MediaTek components, including the thermal driver and video driver, could enable a local malicious application to execute 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: N/A. Android ID: A-31791148. References: MT-ALPS02982181. **Reference: CVE-2016-8448**	https://source.android.com/security/bulletin/01-01-2017.html	O-GOO-ANDRO-190117/201
Execute Code	12-01-2017	7.6	An elevation of privilege vulnerability in MediaTek components, including the thermal driver and video driver, could enable a local malicious application to execute 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: N/A. Android ID: A-31749463. References: MT-	https://source.android.com/security/bulletin/01-01-2017.html	O-GOO-ANDRO-190117/202

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

			ALPS02968886. **Reference: CVE-2016-8447**		
Execute Code	12-01-2017	7.6	An elevation of privilege vulnerability in MediaTek components, including the thermal driver and video driver, could enable a local malicious application to execute 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: N/A. Android ID: A-31747749. References: MT-ALPS02968909. **Reference: CVE-2016-8446**	https://source.android.com/security/bulletin/01-01-2017.html	O-GOO-ANDRO-190117/203
Execute Code	12-01-2017	7.6	An elevation of privilege vulnerability in MediaTek components, including the thermal driver and video driver, could enable a local malicious application to execute 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: N/A. Android ID: A-31747590. References: MT-ALPS02968983. **Reference: CVE-2016-8445**	https://source.android.com/security/bulletin/01-01-2017.html	O-GOO-ANDRO-190117/204
Execute Code	12-01-2017	9.3	An elevation of privilege vulnerability in the MediaTek driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as Critical due to the possibility of a local permanent device compromise, which may require reflashing the operating system to repair the device. Product: Android. Versions: N/A. Android ID: A-31750190.	https://source.android.com/security/bulletin/01-01-2017.html	O-GOO-ANDRO-190117/205

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

			References: MT-ALPS02974192. **Reference: CVE-2016-8433**		
Execute Code	12-01-2017	9.3	An elevation of privilege vulnerability in the Qualcomm bootloader could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as Critical due to the possibility of a local permanent device compromise, which may require reflashing the operating system to repair the device. Product: Android. Versions: N/A. Android ID: A-31399736. References: QC-CR#1000546. **Reference: CVE-2016-8423**	https://source.android.com/security/bulletin/01-01-2017.html	O-GOO-ANDRO-190117/206
Execute Code	12-01-2017	9.3	An elevation of privilege vulnerability in the Qualcomm bootloader could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as Critical due to the possibility of a local permanent device compromise, which may require reflashing the operating system to repair the device. Product: Android. Versions: N/A. Android ID: A-31471220. References: QC-CR#979426. **Reference: CVE-2016-8422**	https://source.android.com/security/bulletin/01-01-2017.html	O-GOO-ANDRO-190117/207
Gain Information	12-01-2017	4.3	Information disclosure vulnerability in the MediaTek video driver could enable a local malicious application to access data outside of its permission levels. This issue is rated as High because it could be used to access sensitive data without explicit user permission. Product: Android. Versions: N/A. Android ID: A-31249105. **Reference: CVE-2016-8396**	https://source.android.com/security/bulletin/2016-12-01.html	O-GOO-ANDRO-190117/208
Execute Code	12-01-2017	7.6	An elevation of privilege	https://sou	O-GOO-

			vulnerability in the MediaTek I2C driver could enable a local malicious application to execute 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: N/A. Android ID: A-31224428. References: MT-ALPS02943467. **Reference: CVE-2016-6788**	rce.android.com/security/bulletin/2016-12-01.html	ANDRO-190117/209
Execute Code	12-01-2017	9.3	An elevation of privilege vulnerability in the MediaTek driver could enable a local malicious application to execute 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: N/A. Android ID: A-31350755. References: MT-ALPS02961424. **Reference: CVE-2016-6784**	https://source.android.com/security/bulletin/2016-12-01.html	O-GOO-ANDRO-190117/210
Bypass; Gain Information	12-01-2017	2.6	Information disclosure vulnerability in Package Manager could enable a local malicious application to bypass operating system protections that isolate application data from other applications. This issue is rated as Moderate because it first requires compromising a privileged process. Product: Android. Versions: 7.0. Android ID: A-31251489. **Reference: CVE-2016-6774**	https://source.android.com/security/bulletin/2016-12-01.html	O-GOO-ANDRO-190117/211
Bypass	12-01-2017	6.8	An elevation of privilege vulnerability in Telephony could enable a local malicious application to access system functions beyond its access level. This issue is rated as Moderate	https://source.android.com/security/bulletin/2016-12-01.html	O-GOO-ANDRO-190117/212

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

			because it is a local bypass of restrictions on a constrained process. Product: Android. Versions: 6.0, 6.0.1, 7.0. Android ID: A-31566390. **Reference: CVE-2016-6771**		
Google; Linux					
Android/Linux Kernel Android is a mobile operating system developed by Google, based on the Linux kernel and designed primarily for touch-screen mobile devices/ Linux Kernel in a Nutshell is a comprehensive overview of kernel configuration and building, a critical task for Linux users and administrators.					
Execute Code	12-01-2017	9.3	An elevation of privilege vulnerability in the Qualcomm video driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as Critical due to the possibility of a local permanent device compromise, which may require reflashing the operating system to repair the device. Product: Android. Versions: Kernel-3.18. Android ID: A-32450261. References: QC-CR#1007860. **Reference: CVE-2016-8436**	https://source.android.com/security/bulletin/01-01-2017.html	O-GOO-ANDRO-190117/213
Intel					
Ethernet Controler X710 Firmware; Ethernet Controler Xl710 Firmware NA					
Denial of Service	09-01-2017	4.3	A Denial of Service in Intel Ethernet Controller's X710/XL710 with Non-Volatile Memory Images before version 5.05 allows a remote attacker to stop the controller from processing network traffic working under certain network use conditions. **Reference: CVE-2016-8106**	https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00063&languageid=en-fr	O-INT-ETHER-190117/214
Linux					
Linux Kernel Linux Kernel in a Nutshell is a comprehensive overview of kernel configuration and building, a critical task for Linux users and administrators.					

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	05-01-2017	7.2	The ring_buffer_resize function in kernel/trace/ring_buffer.c in the profiling subsystem in the Linux kernel before 4.6.1 mishandles certain integer calculations, which allows local users to gain privileges by writing to the /sys/kernel/debug/tracing/buffer_size_kb file. **Reference: CVE-2016-9754**	https://github.com/torvalds/linux/commit/59643d1535eb220668692a5359de22545af579f6	O-LIN-LINUX-190117/215
Execute Code	12-01-2017	7.6	An elevation of privilege vulnerability in the Qualcomm sound driver could enable a local malicious application to execute 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. Android ID: A-32450563. References: QC-CR#880388. **Reference: CVE-2016-8450**	https://source.android.com/security/bulletin/01-01-2017.html	O-LIN-LINUX-190117/216
Execute Code	12-01-2017	7.6	An elevation of privilege vulnerability in the NVIDIA GPU driver could enable a local malicious application to execute 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. Android ID: A-31798848. References: N-CVE-2016-8449. **Reference: CVE-2016-8449**	https://source.android.com/security/bulletin/01-01-2017.html	O-LIN-LINUX-190117/217
Execute Code	12-01-2017	7.6	An elevation of privilege vulnerability in the Qualcomm camera could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a	https://source.android.com/security/bulletin/01-01-2017.html	O-LIN-LINUX-190117/218

			privileged process. Product: Android. Versions: Kernel-3.10. Android ID: A-31243641. References: QC-CR#1074310. **Reference: CVE-2016-8444**		
NA	12-01-2017	7.2	Possible unauthorized memory access in the hypervisor. Incorrect configuration provides access to subsystem page tables. Product: Android. Versions: Kernel 3.18. Android ID: A-32576499. References: QC-CR#964185. **Reference: CVE-2016-8443**	https://source.android.com/security/bulletin/01-01-2017.html	O-LIN-LINUX-190117/219
NA	12-01-2017	7.2	Possible unauthorized memory access in the hypervisor. Lack of input validation could allow hypervisor memory to be accessed by the HLOS. Product: Android. Versions: Kernel 3.18. Android ID: A-31625910. QC-CR#1038173. **Reference: CVE-2016-8442**	https://source.android.com/security/bulletin/01-01-2017.html	O-LIN-LINUX-190117/220
Overflow	12-01-2017	7.2	Possible buffer overflow in the hypervisor. Inappropriate usage of a static array could lead to a buffer overrun. Product: Android. Versions: Kernel 3.18. Android ID: A-31625904. References: QC-CR#1027769. **Reference: CVE-2016-8441**	https://source.android.com/security/bulletin/01-01-2017.html	O-LIN-LINUX-190117/221
Overflow	12-01-2017	10	Possible buffer overflow in SMMU system call. Improper input validation in ADSP SID2CB system call may result in hypervisor memory overwrite. Product: Android. Versions: Kernel 3.18. Android ID: A-31625306. References: QC-CR#1036747. **Reference: CVE-2016-8440**	https://source.android.com/security/bulletin/01-01-2017.html	O-LIN-LINUX-190117/222
Overflow	12-01-2017	10	Possible buffer overflow in trust zone access control API. Buffer overflow may occur due to lack of buffer size checking. Product:	https://source.android.com/security/bulletin	O-LIN-LINUX-190117/223

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

			Android. Versions: Kernel 3.18. Android ID: A-31625204. References: QC-CR#1027804. **Reference: CVE-2016-8439**	/01-01-2017.html	
Overflow; Bypass	12-01-2017	10	Integer overflow leading to a TOCTOU condition in hypervisor PIL. An integer overflow exposes a race condition that may be used to bypass (Peripheral Image Loader) PIL authentication. Product: Android. Versions: Kernel 3.18. Android ID: A-31624565. References: QC-CR#1023638. **Reference: CVE-2016-8438**	https://source.android.com/security/bulletin/01-01-2017.html	O-LIN-LINUX-190117/224
NA	12-01-2017	10	Improper input validation in Access Control APIs. Access control API may return memory range checking incorrectly. Product: Android. Versions: Kernel 3.18. Android ID: A-31623057. References: QC-CR#1009695. **Reference: CVE-2016-8437**	https://source.android.com/security/bulletin/01-01-2017.html	O-LIN-LINUX-190117/225
Execute Code	12-01-2017	9.3	An elevation of privilege vulnerability in the NVIDIA GPU driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as Critical due to the possibility of a local permanent device compromise, which may require reflashing the operating system to repair the device. Product: Android. Versions: Kernel-3.18. Android ID: A-32700935. References: N-CVE-2016-8435. **Reference: CVE-2016-8435**	https://source.android.com/security/bulletin/01-01-2017.html	O-LIN-LINUX-190117/226
Execute Code	12-01-2017	9.3	An elevation of privilege vulnerability in the Qualcomm GPU driver could enable a local malicious application to execute arbitrary code within the	https://source.android.com/security/bulletin/01-01-	O-LIN-LINUX-190117/227

			context of the kernel. This issue is rated as Critical due to the possibility of a local permanent device compromise, which may require reflashing the operating system to repair the device. Product: Android. Versions: Kernel-3.10. Android ID: A-32125137. References: QC-CR#1081855. **Reference: CVE-2016-8434**	2017.html	
Execute Code	12-01-2017	9.3	An elevation of privilege vulnerability in the NVIDIA GPU driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as Critical due to the possibility of a local permanent device compromise, which may require reflashing the operating system to repair the device. Product: Android. Versions: Kernel-3.18. Android ID: A-32447738. References: N-CVE-2016-8432. **Reference: CVE-2016-8432**	https://source.android.com/security/bulletin/01-01-2017.html	O-LIN-LINUX-190117/228
Execute Code	12-01-2017	9.3	An elevation of privilege vulnerability in the NVIDIA GPU driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as Critical due to the possibility of a local permanent device compromise, which may require reflashing the operating system to repair the device. Product: Android. Versions: Kernel-3.18. Android ID: A-32402179. References: N-CVE-2016-8431. **Reference: CVE-2016-8431**	https://source.android.com/security/bulletin/01-01-2017.html	O-LIN-LINUX-190117/229
Execute Code	12-01-2017	9.3	An elevation of privilege vulnerability in the NVIDIA GPU	https://source.android	O-LIN-LINUX-

			driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as Critical due to the possibility of a local permanent device compromise, which may require reflashing the operating system to repair the device. Product: Android. Versions: Kernel-3.10. Android ID: A-32225180. References: N-CVE-2016-8430. **Reference: CVE-2016-8430**	.com/security/bulletin/01-01-2017.html	190117/230
Execute Code	12-01-2017	9.3	An elevation of privilege vulnerability in the NVIDIA GPU driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as Critical due to the possibility of a local permanent device compromise, which may require reflashing the operating system to repair the device. Product: Android. Versions: Kernel-3.10. Android ID: A-32160775. References: N-CVE-2016-8429. **Reference: CVE-2016-8429**	https://source.android.com/security/bulletin/01-01-2017.html	O-LIN-LINUX-190117/231
Execute Code	12-01-2017	9.3	An elevation of privilege vulnerability in the NVIDIA GPU driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as Critical due to the possibility of a local permanent device compromise, which may require reflashing the operating system to repair the device. Product: Android. Versions: Kernel-3.10. Android ID: A-31993456. References: N-CVE-2016-8428.	https://source.android.com/security/bulletin/01-01-2017.html	O-LIN-LINUX-190117/232

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-2016-8428		
Execute Code	12-01-2017	9.3	An elevation of privilege vulnerability in the NVIDIA GPU driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as Critical due to the possibility of a local permanent device compromise, which may require reflashing the operating system to repair the device. Product: Android. Versions: Kernel-3.10. Android ID: A-31799885. References: N-CVE-2016-8427. **Reference: CVE-2016-8427**	https://source.android.com/security/bulletin/01-01-2017.html	O-LIN-LINUX-190117/233
Execute Code	12-01-2017	9.3	An elevation of privilege vulnerability in the NVIDIA GPU driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as Critical due to the possibility of a local permanent device compromise, which may require reflashing the operating system to repair the device. Product: Android. Versions: Kernel-3.10. Android ID: A-31799206. References: N-CVE-2016-8426. **Reference: CVE-2016-8426**	https://source.android.com/security/bulletin/01-01-2017.html	O-LIN-LINUX-190117/234
Execute Code	12-01-2017	9.3	An elevation of privilege vulnerability in the NVIDIA GPU driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as Critical due to the possibility of a local permanent device compromise, which may require reflashing the operating system to repair the device. Product: Android. Versions:	https://source.android.com/security/bulletin/01-01-2017.html	O-LIN-LINUX-190117/235

			Kernel-3.10. Android ID: A-31797770. References: N-CVE-2016-8425. **Reference: CVE-2016-8425**		
Execute Code	12-01-2017	9.3	An elevation of privilege vulnerability in the NVIDIA GPU driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as Critical due to the possibility of a local permanent device compromise, which may require reflashing the operating system to repair the device. Product: Android. Versions: Kernel-3.10. Android ID: A-31606947. References: N-CVE-2016-8424. **Reference: CVE-2016-8424**	https://source.android.com/security/bulletin/01-01-2017.html	O-LIN-LINUX-190117/236
Execute Code	12-01-2017	7.6	An elevation of privilege vulnerability in the Qualcomm Wi-Fi driver could enable a local malicious application to execute 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-31750554. References: QC-CR#1079596. **Reference: CVE-2016-8415**	https://source.android.com/security/bulletin/01-01-2017.html	O-LIN-LINUX-190117/237
Execute Code	12-01-2017	7.6	An elevation of privilege vulnerability in the Qualcomm camera could enable a local malicious application to execute 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-	https://source.android.com/security/bulletin/01-01-2017.html	O-LIN-LINUX-190117/238

			31225246. References: QC-CR#1071891. **Reference: CVE-2016-8412**		
Gain Information	12-01-2017	4.3	Information disclosure vulnerability in kernel components including the ION subsystem, Binder, USB driver and networking subsystem 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-31651010. **Reference: CVE-2016-8405**	https://source.android.com/security/bulletin/2016-12-01.html	O-LIN-LINUX-190117/239
Gain Information	12-01-2017	4.3	Information disclosure vulnerability in the NVIDIA librm library (libnvrm) could enable a local malicious application to access data outside of its permission levels. This issue is rated as Moderate because it could be used to access sensitive data without permission. Product: Android. Versions: Kernel-3.18. Android ID: A-31251599. References: N-CVE-2016-8400. **Reference: CVE-2016-8400**	https://source.android.com/security/bulletin/2016-12-01.html	O-LIN-LINUX-190117/240
Execute Code	12-01-2017	7.6	An elevation of privilege vulnerability in the kernel networking subsystem could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as Moderate because it first requires compromising a privileged process and current compiler optimizations restrict access to the vulnerable code. Product: Android. Versions:	https://source.android.com/security/bulletin/2016-12-01.html	O-LIN-LINUX-190117/241

			Kernel-3.10, Kernel-3.18. Android ID: A-31349935. **Reference: CVE-2016-8399**		
NA	12-01-2017	10	Unauthenticated messages processed by the UE. Certain NAS messages are processed when no EPS security context exists in the UE. Product: Android. Versions: Kernel 3.18. Android ID: A-31548486. References: QC-CR#877705. **Reference: CVE-2016-8398**	https://source.android.com/security/bulletin/01-01-2017.html	O-LIN-LINUX-190117/242
Denial of Service	12-01-2017	7.1	A denial of service vulnerability in the NVIDIA camera driver could enable an attacker to cause a local permanent denial of service, which may require reflashing the operating system to repair the device. This issue is rated as High due to the possibility of local permanent denial of service. Product: Android. Versions: Kernel-3.10. Android ID: A-31403040. References: N-CVE-2016-8395. **Reference: CVE-2016-8395**	https://source.android.com/security/bulletin/2016-12-01.html	O-LIN-LINUX-190117/243
Execute Code	12-01-2017	7.6	An elevation of privilege vulnerability in the Synaptics touchscreen driver could enable a local malicious application to execute 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. Android ID: A-31913197. **Reference: CVE-2016-8394**	https://source.android.com/security/bulletin/2016-12-01.html	O-LIN-LINUX-190117/244
Execute Code	12-01-2017	7.6	An elevation of privilege vulnerability in the Synaptics touchscreen driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it	https://source.android.com/security/bulletin/2016-12-01.html	O-LIN-LINUX-190117/245

			first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10. Android ID: A-31911920. **Reference: CVE-2016-8393**		
Execute Code	12-01-2017	7.6	An elevation of privilege vulnerability in the Qualcomm sound driver could enable a local malicious application to execute 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-31385862. References: QC-CR#1073136. **Reference: CVE-2016-8392**	https://source.android.com/security/bulletin/2016-12-01.html	O-LIN-LINUX-190117/246
Execute Code	12-01-2017	7.6	An elevation of privilege vulnerability in the Qualcomm sound driver could enable a local malicious application to execute 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-31253255. References: QC-CR#1072166. **Reference: CVE-2016-8391**	https://source.android.com/security/bulletin/2016-12-01.html	O-LIN-LINUX-190117/247
Execute Code	12-01-2017	7.6	An elevation of privilege vulnerability in the Qualcomm sound driver could enable a local malicious application to execute 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-31252384. References: QC-	https://source.android.com/security/bulletin/2016-12-01.html	O-LIN-LINUX-190117/248

			CR#1071809. **Reference: CVE-2016-6791**		
Gain Information	12-01-2017	2.6	Information disclosure vulnerability in Qualcomm components including the camera driver and 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-3.10, Kernel-3.18. Android ID: A-30148242. References: QC-CR#1052821. **Reference: CVE-2016-6757**	https://source.android.com/security/bulletin/2016-12-01.html	O-LIN-LINUX-190117/249
Gain Information	12-01-2017	2.6	Information disclosure vulnerability in Qualcomm components including the camera driver and 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-3.10, Kernel-3.18. Android ID: A-29464815. References: QC-CR#1042068. **Reference: CVE-2016-6756**	https://source.android.com/security/bulletin/2016-12-01.html	O-LIN-LINUX-190117/250
Execute Code	12-01-2017	7.6	An elevation of privilege vulnerability in the Qualcomm camera driver could enable a local malicious application to execute 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-30740545. References: QC-CR#1065916.	https://source.android.com/security/bulletin/2016-12-01.html	O-LIN-LINUX-190117/251

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-2016-6755		
Microsoft					
Windows 7;Windows Server 2008;Windows Vista Microsoft Windows (or simply Windows) is a metafamily of graphical operating systems developed, marketed, and sold by Microsoft.					
Denial of Service	10-01-2017	7.8	The Local Security Authority Subsystem Service (LSASS) in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allows remote attackers to cause a denial of service (reboot) via a crafted authentication request, aka "Local Security Authority Subsystem Service Denial of Service Vulnerability." **Reference: CVE-2017-0004**	NA	O-MIC-WINDO-190117/252
Netgear					
Arlo Base Station Firmware;Arlo Q Camera Firmware;Arlo Q Plus Camera Firmware NA					
NA	04-01-2017	9.3	NETGEAR Arlo base stations with firmware 1.7.5_6178 and earlier, Arlo Q devices with firmware 1.8.0_5551 and earlier, and Arlo Q Plus devices with firmware 1.8.1_6094 and earlier use a pattern of adjective, noun, and three-digit number for the customized password, which makes it easier for remote attackers to obtain access via a dictionary attack. **Reference: CVE-2016-10116**	NA	O-NET-ARLO - 190117/253
NA	04-01-2017	10	NETGEAR Arlo base stations with firmware 1.7.5_6178 and earlier, Arlo Q devices with firmware 1.8.0_5551 and earlier, and Arlo Q Plus devices with firmware 1.8.1_6094 and earlier have a default password of 12345678, which makes it easier for remote attackers to obtain access after a factory	NA	O-NET-ARLO - 190117/254

			reset or in a factory configuration. **Reference: CVE-2016-10115**		
Fvs318gv2 Firmware;Fvs318n Firmware;Fvs336gv3 Firmware;Srx5308 Firmware NA					
Directory Traversal	03-01-2017	4	Directory traversal vulnerability in scgi-bin/platform.cgi on NETGEAR FVS336Gv3, FVS318N, FVS318Gv2, and SRX5308 devices with firmware before 4.3.3-8 allows remote authenticated users to read arbitrary files via a .. (dot dot) in the thispage parameter, as demonstrated by reading the /etc/shadow file. **Reference: CVE-2016-10106**	http://kb.netgear.com/30739/Path-Traversal-Attack-Security-Vulnerability	O-NET-FVS31-190117/255
Samsung					
Samsung Mobile Samsung is a South Korean multinational conglomerate company headquartered in Samsung Town, Seoul.					
NA	09-01-2017	7.1	Installing a zero-permission Android application on certain Samsung Android devices with KK(4.4), L(5.0/5.1), and M(6.0) software can continually crash the system_server process in the Android OS. The zero-permission app will create an active install session for a separate app that it has embedded within it. The active install session of the embedded app is performed using the android.content.pm.PackageInstaller class and its nested classes in the Android API. The active install session will write the embedded APK file to the /data/app directory, but the app will not be installed since third-party applications cannot programmatically install apps.	http://security.samsungmobile.com/smrupdate.html#SMR-JAN-2017	O-SAM-SAMSU-190117/256

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

			Samsung has modified AOSP in order to accelerate the parsing of APKs by introducing the com.android.server.pm.PackagePrefetcher class and its nested classes. These classes will parse the APKs present in the /data/app directory and other directories, even if the app is not actually installed. The embedded APK that was written to the /data/app directory via the active install session has a very large but valid AndroidManifest.xml file. Specifically, the AndroidManifest.xml file contains a very large string value for the name of a permission-tree that it declares. When system_server tries to parse the APK file of the embedded app from the active install session, it will crash due to an uncaught error (i.e., java.lang.OutOfMemoryError) or an uncaught exception (i.e., std::bad_alloc) because of memory constraints. The Samsung Android device will encounter a soft reboot due to a system_server crash, and this action will keep repeating since parsing the APKs in the /data/app directory as performed by the system_server process is part of the normal boot process. The Samsung ID is SVE-2016-6917. **Reference: CVE-2017-5217**		
NA	12-01-2017	7.8	Samsung Note devices with KK(4.4), L(5.0/5.1), and M(6.0) software allow attackers to crash the system by creating an arbitrarily large number of	http://security.samsungmobile.com/smrupdate.html#S	O-SAM-SAMSU-190117/257

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

			active VR service threads. The Samsung ID is SVE-2016-7650. **Reference: CVE-2017-5351**	MR-JAN-2017	
NA	12-01-2017	5	Samsung Note devices with L(5.0/5.1), M(6.0), and N(7.0) software allow attackers to crash systemUI by leveraging incomplete exception handling. The Samsung ID is SVE-2016-7122. **Reference: CVE-2017-5350**	http://security.samsungmobile.com/smrupdate.html#SMR-JAN-2017	O-SAM-SAMSU-190117/258
Trane					
Comfortlink Ii Firmware NA					
Execute Code; Overflow	06-01-2017	10	Exploitable remote code execution vulnerability exists in the Trane ComfortLink II firmware version 2.0.2 in DSS service. An attacker who can connect to the DSS service on the Trane ComfortLink II device can send an overly long REG request that can overflow a fixed size stack buffer, resulting in arbitrary code execution. **Reference: CVE-2015-2868**	NA	O-TRA-COMFO-190117/259
NA	06-01-2017	10	A design flaw in the Trane ComfortLink II SCC firmware version 2.0.2 service allows remote attackers to take complete control of the system. **Reference: CVE-2015-2867**	NA	O-TRA-COMFO-190117/260