National Critical Information Infrastructure Protection Centre
CVE Report
01-31 May 2017 Vol. 04 No. 08

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Application (A)					
21st Century Insurance					
21st Century Insurance					
Gain Information	05-05-2017	4.3	The 21st Century Insurance app 10.0.0 for iOS does not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate. **CVE ID: CVE-2017-5919**	https://medium.com/@chronic_9612/follow-up-76-popular-apps-confirmed-vulnerable-to-silent-interception-of-tls-protected-data-64185035029f	A-21S-21ST - 230617 /01
7-zip					
7-zip					
Gain Privileges	22-05-2017	6.8	Untrusted search path vulnerability in 7 Zip for Windows 16.02 and earlier allows remote attackers to gain privileges via a Trojan horse DLL in an unspecified directory. **CVE ID: CVE-2016-7804**	http://www.7-zip.org/history.txt	A-7-Z-7-ZIP-230617 /02
Accellion					
File Transfer Appliance					
XSS	05-05-2017	4.3	An issue was discovered on Accellion FTA devices before FTA_9_12_180. There is XSS in home/seos/courier/smtpg_add.html with the param parameter. **CVE ID: CVE-2017-8795**	https://gist.github.com/anonymous/32e2894fa29176f3f32cb2b2bb7c24cb	A-ACC-FILE - 230617 /03
XSS	05-05-2017	4.3	An issue was discovered on Accellion FTA devices before FTA_9_12_180. There is XSS in home/seos/courier/user_add.html with the param parameter.	https://gist.github.com/anonymous/32e2894fa29176f3f32cb2b2bb7c24	A-ACC-FILE - 230617 /04

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

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

			CVE ID: CVE-2017-8792	cb	
NA	05-05-2017	4.3	An issue was discovered on Accellion FTA devices before FTA_9_12_180. There is a home/seos/courier/login.html auth_params CRLF attack vector. **CVE ID: CVE-2017-8791**	https://gist.github.com/anonymous/32e2894fa29176f3f32cb2b2bb7c24cb	A-ACC-FILE - 230617/05
NA	05-05-2017	4.3	An issue was discovered on Accellion FTA devices before FTA_9_12_180. There is a CRLF vulnerability in settings_global_text_edit.php allowing ?display=x%0Dnewline attacks. **CVE ID: CVE-2017-8788**	https://gist.github.com/anonymous/32e2894fa29176f3f32cb2b2bb7c24cb	A-ACC-FILE - 230617/06
XSS Bypass	05-05-2017	4.3	An issue was discovered on Accellion FTA devices before FTA_9_12_180. There is XSS in courier/1000@/index.html with the auth_params parameter. The device tries to use internal WAF filters to stop specific XSS Vulnerabilities. However, these can be bypassed by using some modifications to the payloads, e.g., URL encoding. **CVE ID: CVE-2017-8760**	https://gist.github.com/anonymous/32e2894fa29176f3f32cb2b2bb7c24cb	A-ACC-FILE - 230617/07
XSS	05-05-2017	4.3	An issue was discovered on Accellion FTA devices before FTA_9_12_180. courier/1000@/oauth/playground/callback.html allows XSS with a crafted URI. **CVE ID: CVE-2017-8304**	https://gist.github.com/anonymous/32e2894fa29176f3f32cb2b2bb7c24cb	A-ACC-FILE - 230617/08
NA	05-05-2017	6.4	An issue was discovered on Accellion FTA devices before FTA_9_12_180. Because a regular expression (intended to match local https URLs) lacks an initial ^ character, courier/web/1000@/wmProgressval.html allows SSRF attacks with a file:///etc/passwd#https:// URL pattern. **CVE ID: CVE-2017-8794**	https://gist.github.com/anonymous/32e2894fa29176f3f32cb2b2bb7c24cb	A-ACC-FILE - 230617/09
Bypass	05-05-2017	6.8	An issue was discovered on Accellion FTA devices before FTA_9_12_180. By sending a POST request to	https://gist.github.com/anonymous/32e28	A-ACC-FILE - 230617

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

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

			home/seos/courier/web/wmProgressstat.html.php with an attacker domain in the acallow parameter, the device will respond with an Access-Control-Allow-Origin header allowing the attacker to have site access with a bypass of the Same Origin Policy. **CVE ID: CVE-2017-8793**	94fa29176f3f32cb2b2bb7c24cb	/10
Sql	05-05-2017	7.5	An issue was discovered on Accellion FTA devices before FTA_9_12_180. Because mysql_real_escape_string is misused, seos/courier/communication_p2p.php allows SQL injection with the app_id parameter. **CVE ID: CVE-2017-8796**	https://gist.github.com/anonymous/32e2894fa29176f3f32cb2b2bb7c24cb	A-ACC-FILE - 230617/11
NA	05-05-2017	7.5	An issue was discovered on Accellion FTA devices before FTA_9_12_180. The home/seos/courier/ldaptest.html POST parameter "filter" can be used for LDAP Injection. **CVE ID: CVE-2017-8790**	https://gist.github.com/anonymous/32e2894fa29176f3f32cb2b2bb7c24cb	A-ACC-FILE - 230617/12
Sql	05-05-2017	7.5	An issue was discovered on Accellion FTA devices before FTA_9_12_180. A report_error.php?year='payload SQL injection vector exists. **CVE ID: CVE-2017-8789**	https://gist.github.com/anonymous/32e2894fa29176f3f32cb2b2bb7c24cb	A-ACC-FILE - 230617/13
Execute Code	05-05-2017	7.5	An issue was discovered on Accellion FTA devices before FTA_9_12_180. seos/1000/find.api allows Remote Code Execution with shell metacharacters in the method parameter. **CVE ID: CVE-2017-8303**	https://gist.github.com/anonymous/32e2894fa29176f3f32cb2b2bb7c24cb	A-ACC-FILE - 230617/14
Adobe					
Experience Manager Forms					
Gain Information	09-05-2017	5	Adobe Experience Manager Forms versions 6.2, 6.1, 6.0 have an information disclosure vulnerability resulting from abuse of the pre-	https://helpx.adobe.com/security/products/aem-	A-ADO-EXPER-230617/15

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

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

			population service in AEM Forms. **CVE ID: CVE-2017-3067**	forms/apsb17-16.html	
Flash Player					
Execute Code Overflow Memory Corruption	09-05-2017	10	Adobe Flash Player versions 25.0.0.148 and earlier have an exploitable memory corruption vulnerability in the Graphics class. Successful exploitation could lead to arbitrary code execution. **CVE ID: CVE-2017-3074**	https://helpx.adobe.com/security/products/flash-player/apsb17-15.html	A-ADO-FLASH-230617/16
Execute Code Overflow Memory Corruption	09-05-2017	10	Adobe Flash Player versions 25.0.0.148 and earlier have an exploitable use after free vulnerability when handling multiple mask properties of display objects, aka memory corruption. Successful exploitation could lead to arbitrary code execution. **CVE ID: CVE-2017-3073**	https://helpx.adobe.com/security/products/flash-player/apsb17-15.html	A-ADO-FLASH-230617/17
Execute Code Overflow Memory Corruption	09-05-2017	10	Adobe Flash Player versions 25.0.0.148 and earlier have an exploitable memory corruption vulnerability in the BitmapData class. Successful exploitation could lead to arbitrary code execution. **CVE ID: CVE-2017-3072**	https://helpx.adobe.com/security/products/flash-player/apsb17-15.html	A-ADO-FLASH-230617/18
Execute Code	09-05-2017	10	Adobe Flash Player versions 25.0.0.148 and earlier have an exploitable use after free vulnerability when masking display objects. Successful exploitation could lead to arbitrary code execution. **CVE ID: CVE-2017-3071**	https://helpx.adobe.com/security/products/flash-player/apsb17-15.html	A-ADO-FLASH-230617/19
Execute Code Overflow Memory Corruption	09-05-2017	10	Adobe Flash Player versions 25.0.0.148 and earlier have an exploitable memory corruption vulnerability in the ConvolutionFilter class. Successful exploitation could lead to arbitrary code execution. **CVE ID: CVE-2017-3070**	https://helpx.adobe.com/security/products/flash-player/apsb17-15.html	A-ADO-FLASH-230617/20
Execute Code Overflow Memory	09-05-2017	10	Adobe Flash Player versions 25.0.0.148 and earlier have an exploitable memory corruption	https://helpx.adobe.com/security/products	A-ADO-FLASH-230617

Corruption			vulnerability in the BlendMode class. Successful exploitation could lead to arbitrary code execution. **CVE ID: CVE-2017-3069**	/flash-player/apsb17-15.html	/21
Execute Code Overflow Memory Corruption	09-05-2017	10	Adobe Flash Player versions 25.0.0.148 and earlier have an exploitable memory corruption vulnerability in the Advanced Video Coding engine. Successful exploitation could lead to arbitrary code execution. **CVE ID: CVE-2017-3068**	https://helpx.adobe.com/security/products/flash-player/apsb17-15.html	A-ADO-FLASH-230617/22
Adodb Project					
Adodb					
XSS	12-05-2017	4.3	Cross-site scripting vulnerability in ADOdb versions prior to 5.20.6 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors. **CVE ID: CVE-2016-4855**	https://github.com/ADOdb/ADOdb/issues/274	A-ADO-ADODB-230617/23
Advantech					
Webaccess					
Gain Information	02-05-2017	4	upAdminPg.asp in Advantech WebAccess before 8.1_20160519 allows remote authenticated administrators to obtain sensitive password information via unspecified vectors. **CVE ID: CVE-2016-5810**	NA	A-ADV-WEBAC-230617/24
Directory Traversal	05-05-2017	5.5	An Absolute Path Traversal issue was discovered in Advantech WebAccess Version 8.1 and prior. The absolute path traversal vulnerability has been identified, which may allow an attacker to traverse the file system to access restricted files or directories. **CVE ID: CVE-2017-7929**	NA	A-ADV-WEBAC-230617/25
Alienvault					
Open Source Security Information Management					
Execute Code	23-05-2017	6.5	The asset discovery scanner in AlienVault OSSIM before 5.0.1 allows remote authenticated users to execute arbitrary commands via the	https://www.alienvault.com/forums/discussion/5127/	A-ALI-OPEN-230617/26

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

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

			assets array parameter to netscan/do_scan.php. **CVE ID: CVE-2015-4046**		
Open Source Security Information Management					
Gain Privileges	23-05-2017	7.2	The sudoers file in the asset discovery scanner in AlienVault OSSIM before 5.0.1 allows local users to gain privileges via a crafted nmap script. **CVE ID: CVE-2015-4045**	https://www.alienvault.com/forums/discussion/5127/	A-ALI-OPEN - 230617/27
Allen Disk Project					
Allen Disk					
NA	31-05-2017	4	SSRF vulnerability in remotedownload.php in Allen Disk 1.6 allows remote authenticated users to conduct port scans and access intranet servers via a crafted file parameter. **CVE ID: CVE-2017-9307**	https://github.com/s3131212/allendisk/issues/20	A-ALL-ALLEN-230617/28
CSRF	08-05-2017	4.3	Allen Disk 1.6 has CSRF in setpass.php with an impact of changing a password. **CVE ID: CVE-2017-8848**	https://github.com/s3131212/allendisk/issues/16	A-ALL-ALLEN-230617/29
XSS	08-05-2017	4.3	Allen Disk 1.6 has XSS in the id parameter to downfile.php. **CVE ID: CVE-2017-8832**	https://github.com/s3131212/allendisk/commit/37b6a63b85d5ab3ed81141cadc47489d7571664b	A-ALL-ALLEN-230617/30
Bypass	19-05-2017	5	/admin/loginc.php in Allen Disk 1.6 doesn't check if isset($_SESSION['captcha']['code']) == 1, which leads to CAPTCHA bypass by emptying $_POST['captcha']. **CVE ID: CVE-2017-9091**	https://github.com/s3131212/allendisk/issues/23	A-ALL-ALLEN-230617/31
Bypass	19-05-2017	5	reg.php in Allen Disk 1.6 doesn't check if isset($_SESSION['captcha']['code'])==1, which makes it possible to bypass the CAPTCHA via an empty $_POST['captcha'].	https://github.com/s3131212/allendisk/issues/25	A-ALL-ALLEN-230617/32

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

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

			CVE ID: CVE-2017-9090		
America's First Federal Credit Union					
America's First Fcu Mobile Banking					
Gain Information	05-05-2017	4.3	The America's First Federal Credit Union (FCU) Mobile Banking app 3.1.0 for iOS does not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate. **CVE ID: CVE-2017-5916**	https://medium.com/@chronic_9612/follow-up-76-popular-apps-confirmed-vulnerable-to-silent-interception-of-tls-protected-data-64185035029f	A-AME-AMERI-230617/33
Apache					
Ambari					
Gain Information	15-05-2017	4	In Ambari 2.2.2 through 2.4.2 and Ambari 2.5.0, sensitive data may be stored on disk in temporary files on the Ambari Server host. The temporary files are readable by any user authenticated on the host. **CVE ID: CVE-2017-5655**	https://cwiki.apache.org/confluence/display/AMBARI/Ambari+Vulnerabilities#AmbariVulnerabilities-FixedinAmbari2.5.1	A-APA-AMBAR-230617/34
NA	12-05-2017	5	In Ambari 2.4.x (before 2.4.3) and Ambari 2.5.0, an authorized user of the Ambari Hive View may be able to gain unauthorized read access to files on the host where the Ambari server executes. **CVE ID: CVE-2017-5654**	https://cwiki.apache.org/confluence/display/AMBARI/Ambari+Vulnerabilities#AmbariVulnerabilities-FixedinAmbari2.5.1	A-APA-AMBAR-230617/35
CSRF	22-05-2017	6	Several REST service endpoints of Apache Archiva are not protected against Cross Site Request Forgery (CSRF) attacks. A malicious site opened in the same browser as the	http://archiva.apache.org/security.html#CVE-2017-5657	A-APA-ARCHI-230617/36

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

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

			archiva site, may send an HTML response that performs arbitrary actions on archiva services, with the same rights as the active archiva session (e.g. administrator rights). **CVE ID: CVE-2017-5657**		
Cordova					
NA	09-05-2017	5	Product: Apache Cordova Android 5.2.2 and earlier. The application calls methods of the Log class. Messages passed to these methods (Log.v(), Log.d(), Log.i(), Log.w(), and Log.e()) are stored in a series of circular buffers on the device. By default, a maximum of four 16 KB rotated logs are kept in addition to the current log. The logged data can be read using Logcat on the device. When using platforms prior to Android 4.1 (Jelly Bean), the log data is not sandboxed per application; any application installed on the device has the capability to read data logged by other applications. **CVE ID: CVE-2016-6799**	NA	A-APA-CORDO-230617/37
Cxf Fediz					
CSRF	16-05-2017	6.8	Apache CXF Fediz ships with an OpenId Connect (OIDC) service which has a Client Registration Service, which is a simple web application that allows clients to be created, deleted, etc. A CSRF (Cross Style Request Forgery) style vulnerability has been found in this web application in Apache CXF Fediz prior to 1.4.0 and 1.3.2, meaning that a malicious web application could create new clients, or reset secrets, etc, after the admin user has logged on to the client registration service and the session is still active. **CVE ID: CVE-2017-7662**	http://cxf.apache.org/security-advisories.data/CVE-2017-7662.txt.asc	A-APA-CXF F-230617/38
CSRF	16-05-2017	6.8	Apache CXF Fediz ships with a	http://cxf.apac	A-APA-

			number of container-specific plugins to enable WS-Federation for applications. A CSRF (Cross Style Request Forgery) style vulnerability has been found in the Spring 2, Spring 3, Jetty 8 and Jetty 9 plugins in Apache CXF Fediz prior to 1.4.0, 1.3.2 and 1.2.4. **CVE ID: CVE-2017-7661**	he.org/security-advisories.data/CVE ID: CVE-2017-7661.txt.asc	CXF F-230617/39
Hive					
NA	30-05-2017	5	Apache Hive (JDBC + HiveServer2) implements SSL for plain TCP and HTTP connections (it supports both transport modes). While validating the server's certificate during the connection setup, the client in Apache Hive before 1.2.2 and 2.0.x before 2.0.1 doesn't seem to be verifying the common name attribute of the certificate. In this way, if a JDBC client sends an SSL request to server abc.com, and the server responds with a valid certificate (certified by CA) but issued to xyz.com, the client will accept that as a valid certificate and the SSL handshake will go through. **CVE ID: CVE-2016-3083**		A-APA-HIVE-230617/40
Juddi					
NA	19-05-2017	5.8	After logging into the portal, the logout jsp page redirects the browser back to the login page after. It is feasible for malicious users to redirect the browser to an unintended web page in Apache jUDDI 3.1.2, 3.1.3, 3.1.4, and 3.1.5 when utilizing the portlets based user interface also known as 'Pluto', 'jUDDI Portal', 'UDDI Portal' or 'uddi-console'. User session data, credentials, and auth tokens are cleared before the redirect. **CVE ID: CVE-2015-5241**	http://juddi.apache.org/security.html	A-APA-JUDDI-230617/41

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

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

Knox					
NA	26-05-2017	4.9	For versions of Apache Knox from 0.2.0 to 0.11.0 - an authenticated user may use a specially crafted URL to impersonate another user while accessing WebHDFS through Apache Knox. This may result in escalated privileges and unauthorized data access. While this activity is audit logged and can be easily associated with the authenticated user, this is still a serious security issue. All users are recommended to upgrade to the Apache Knox 0.12.0 release. **CVE ID: CVE-2017-5646**	NA	A-APA-KNOX-230617/42
Qpid Java					
Gain Information	15-05-2017	5	The Apache Qpid Broker for Java can be configured to use different so called AuthenticationProviders to handle user authentication. Among the choices are the SCRAM-SHA-1 and SCRAM-SHA-256 AuthenticationProvider types. It was discovered that these AuthenticationProviders in Apache Qpid Broker for Java 6.0.x before 6.0.6 and 6.1.x before 6.1.1 prematurely terminate the SCRAM SASL negotiation if the provided user name does not exist thus allowing remote attacker to determine the existence of user accounts. The Vulnerability does not apply to AuthenticationProviders other than SCRAM-SHA-1 and SCRAM-SHA-256. **CVE ID: CVE-2016-8741**	https://issues.apache.org/jira/browse/QPID-7599	A-APA-QPID-230617/43
NA	02-05-2017	4.3	The C client and C-based client bindings in the Apache Qpid Proton library before 0.13.1 on Windows do not properly verify that the server hostname matches a domain name in the subject's Common Name (CN) or subjectAltName field of the X.509	NA	A-APA-QPID-230617/44

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

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

			certificate when using the SChannel-based security layer, which allows man-in-the-middle attackers to spoof servers via an arbitrary valid certificate. **CVE ID: CVE-2016-4467**		
Apple					
Safari					
NA	22-05-2017	4.3	An issue was discovered in certain Apple products. Safari before 10.1.1 is affected. The issue involves the "Safari" component. It allows remote attackers to spoof the address bar via a crafted web site. **CVE ID: CVE-2017-2511**	https://support.apple.com/HT207804	A-APP-SAFAR-230617/45
Artifex					
Ghostscript					
DoS	12-05-2017	4.3	The mark_line_tr function in gxscanc.c in Artifex Ghostscript 9.21 allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted PostScript document. **CVE ID: CVE-2017-8908**	NA	A-ART-GHOST-230617/46
Bypass Gain Information	23-05-2017	4.3	Ghostscript before 9.21 might allow remote attackers to bypass the SAFER mode protection mechanism and consequently read arbitrary files via the use of the .libfile operator in a crafted postscript document. **CVE ID: CVE-2016-7977**	https://bugs.ghostscript.com/show_bug.cgi?id=697169	A-ART-GHOST-230617/47
Execute Code Bypass	23-05-2017	7.5	Ghostscript before 9.21 might allow remote attackers to bypass the SAFER mode protection mechanism and consequently execute arbitrary code by leveraging type confusion in .initialize_dsc_parser. **CVE ID: CVE-2016-7979**	http://git.ghostscript.com/?p=ghostpdl.git;h=875a0095f37626a721c7ff57d606a0f95af03913	A-ART-GHOST-230617/48
Execute Code	23-05-2017	7.5	Use-after-free vulnerability in Ghostscript 9.20 might allow remote attackers to execute arbitrary code via vectors related to a reference leak in .setdevice.	https://bugs.ghostscript.com/show_bug.cgi?id=697179	A-ART-GHOST-230617/49

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

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

			CVE ID: CVE-2016-7978		
Jbig2dec					
NA	24-05-2017	4.3	libjbig2dec.a in Artifex jbig2dec 0.13, as used in MuPDF and Ghostscript, has a NULL pointer dereference in the jbig2_huffman_get function in jbig2_huffman.c. For example, the jbig2dec utility will crash (segmentation fault) when parsing an invalid file. **CVE ID: CVE-2017-9216**		A-ART-JBIG2-230617/50
Atlassian					
Hipchat					
NA	05-05-2017	4.3	Acceptance of invalid/self-signed TLS certificates in Atlassian HipChat before 3.16.2 for iOS allows a man-in-the-middle and/or physically proximate attacker to silently intercept information sent during the login API call. **CVE ID: CVE-2017-8058**	NA	A-ATL-HIPCH-230617/51
Hipchat Server					
Execute Code	05-05-2017	6.5	Atlassian Hipchat Server before 2.2.4 allows remote authenticated users with user level privileges to execute arbitrary code via vectors involving image uploads. **CVE ID: CVE-2017-8080**	https://jira.atlassian.com/browse/HCPUB-2980	A-ATL-HIPCH-230617/52
Sourcetree					
Execute Code	04-05-2017	10	Atlassian SourceTree v2.5c and prior are affected by a command injection in the handling of the sourcetree:// scheme. It will lead to arbitrary OS command execution with a URL substring of sourcetree://cloneRepo/ext:: or sourcetree://checkoutRef/ext:: followed by the command. The Atlassian ID number is SRCTREE-4632. **CVE ID: CVE-2017-8768**		A-ATL-SOURC-230617/53
Authconfig Project					

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

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

Authconfig					
Gain Information	16-05-2017	4	Authconfig version 6.2.8 is vulnerable to an Information exposure while using SSSD to authenticate against remote server resulting in the leak of information about existing usernames. **CVE ID: CVE-2017-7488**	https://bugzilla.redhat.com/show_bug.cgi?id=1441604	A-AUT-AUTHC-230617/54
Autotrace Project					
Autotrace					
DoS	23-05-2017	5	libautotrace.a in AutoTrace 0.31.1 allows remote attackers to cause a denial of service (invalid free), related to the free_bitmap function in bitmap.c:24:5. **CVE ID: CVE-2017-9190**	https://blogs.gentoo.org/ago/2017/05/20/autotrace-multiple-vulnerabilities-the-autotrace-nightmare/	A-AUT-AUTOT-230617/55
DoS	23-05-2017	5	libautotrace.a in AutoTrace 0.31.1 allows remote attackers to cause a denial of service (invalid read and application crash), related to the GET_COLOR function in color.c:16:11. **CVE ID: CVE-2017-9189**	https://blogs.gentoo.org/ago/2017/05/20/autotrace-multiple-vulnerabilities-the-autotrace-nightmare/	A-AUT-AUTOT-230617/56
DoS	23-05-2017	5	libautotrace.a in AutoTrace 0.31.1 allows remote attackers to cause a denial of service (use-after-free and invalid heap read), related to the GET_COLOR function in color.c:16:11. **CVE ID: CVE-2017-9182**	NA	A-AUT-AUTOT-230617/57
DoS	23-05-2017	5	libautotrace.a in AutoTrace 0.31.1 allows remote attackers to cause a denial of service (invalid write and SEGV), related to the ReadImage function in input-bmp.c. **CVE ID: CVE-2017-9181**	https://blogs.gentoo.org/ago/2017/05/20/autotrace-multiple-vulnerabilities-the-autotrace-nightmare/	A-AUT-AUTOT-230617/58
DoS	23-05-2017	5	libautotrace.a in AutoTrace 0.31.1 allows remote attackers to cause a	NA	A-AUT-AUTOT-

			denial of service (invalid read and SEGV), related to the ReadImage function in input-bmp.c:440:14. **CVE ID: CVE-2017-9180**		230617 /59
DoS	23-05-2017	5	libautotrace.a in AutoTrace 0.31.1 allows remote attackers to cause a denial of service (invalid read and SEGV), related to the ReadImage function in input-bmp.c:425:14. **CVE ID: CVE-2017-9179**	https://blogs.gentoo.org/ago/2017/05/20/autotrace-multiple-vulnerabilities-the-autotrace-nightmare/	A-AUT-AUTOT-230617 /60
DoS	23-05-2017	5	libautotrace.a in AutoTrace 0.31.1 allows remote attackers to cause a denial of service (invalid write and SEGV), related to the ReadImage function in input-bmp.c:421:11. **CVE ID: CVE-2017-9178**	https://blogs.gentoo.org/ago/2017/05/20/autotrace-multiple-vulnerabilities-the-autotrace-nightmare/	A-AUT-AUTOT-230617 /61
DoS	23-05-2017	5	libautotrace.a in AutoTrace 0.31.1 allows remote attackers to cause a denial of service (invalid read and SEGV), related to the ReadImage function in input-bmp.c:390:12. **CVE ID: CVE-2017-9177**	https://blogs.gentoo.org/ago/2017/05/20/autotrace-multiple-vulnerabilities-the-autotrace-nightmare/	A-AUT-AUTOT-230617 /62
DoS	23-05-2017	5	libautotrace.a in AutoTrace 0.31.1 allows remote attackers to cause a denial of service (invalid write and SEGV), related to the ReadImage function in input-bmp.c:370:25. **CVE ID: CVE-2017-9176**	https://blogs.gentoo.org/ago/2017/05/20/autotrace-multiple-vulnerabilities-the-autotrace-nightmare/	A-AUT-AUTOT-230617 /63
DoS	23-05-2017	5	libautotrace.a in AutoTrace 0.31.1 allows remote attackers to cause a denial of service (invalid write and SEGV), related to the ReadImage function in input-bmp.c:353:25. **CVE ID: CVE-2017-9175**	https://blogs.gentoo.org/ago/2017/05/20/autotrace-multiple-vulnerabilities-the-autotrace-nightmare/	A-AUT-AUTOT-230617 /64

DoS	23-05-2017	5	libautotrace.a in AutoTrace 0.31.1 allows remote attackers to cause a denial of service (invalid read and SEGV), related to the GET_COLOR function in color.c:21:23. **CVE ID: CVE-2017-9174**	https://blogs.gentoo.org/ago/2017/05/20/autotrace-multiple-vulnerabilities-the-autotrace-nightmare/	A-AUT-AUTOT-230617/65
DoS	23-05-2017	5	libautotrace.a in AutoTrace 0.31.1 allows remote attackers to cause a denial of service (invalid write and SEGV), related to the pnm_load_rawpbm function in input-pnm.c:391:15. **CVE ID: CVE-2017-9159**	https://blogs.gentoo.org/ago/2017/05/20/autotrace-multiple-vulnerabilities-the-autotrace-nightmare/	A-AUT-AUTOT-230617/66
DoS	23-05-2017	5	libautotrace.a in AutoTrace 0.31.1 allows remote attackers to cause a denial of service (invalid write and SEGV), related to the pnm_load_raw function in input-pnm.c:336:11. **CVE ID: CVE-2017-9158**	https://blogs.gentoo.org/ago/2017/05/20/autotrace-multiple-vulnerabilities-the-autotrace-nightmare/	A-AUT-AUTOT-230617/67
DoS	23-05-2017	5	libautotrace.a in AutoTrace 0.31.1 allows remote attackers to cause a denial of service (invalid write and SEGV), related to the pnm_load_ascii function in input-pnm.c:306:14. **CVE ID: CVE-2017-9157**	https://blogs.gentoo.org/ago/2017/05/20/autotrace-multiple-vulnerabilities-the-autotrace-nightmare/	A-AUT-AUTOT-230617/68
DoS	23-05-2017	5	libautotrace.a in AutoTrace 0.31.1 allows remote attackers to cause a denial of service (invalid write and SEGV), related to the pnm_load_ascii function in input-pnm.c:303:12. **CVE ID: CVE-2017-9156**	https://blogs.gentoo.org/ago/2017/05/20/autotrace-multiple-vulnerabilities-the-autotrace-nightmare/	A-AUT-AUTOT-230617/69
DoS	23-05-2017	5	libautotrace.a in AutoTrace 0.31.1 allows remote attackers to cause a denial of service (invalid read and SEGV), related to the	https://blogs.gentoo.org/ago/2017/05/20/autotrace-	A-AUT-AUTOT-230617/70

			input_pnm_reader function in input-pnm.c:243:3. **CVE ID: CVE-2017-9155**	multiple-vulnerabilities-the-autotrace-nightmare/	
DoS	23-05-2017	5	libautotrace.a in AutoTrace 0.31.1 allows remote attackers to cause a denial of service (invalid read and SEGV), related to the GET_COLOR function in color.c:16:11. **CVE ID: CVE-2017-9154**	https://blogs.gentoo.org/ago/2017/05/20/autotrace-multiple-vulnerabilities-the-autotrace-nightmare/	A-AUT-AUTOT-230617/71
NA	23-05-2017	7.5	libautotrace.a in AutoTrace 0.31.1 has a "cannot be represented in type int" issue in input-tga.c:528:63. **CVE ID: CVE-2017-9200**	https://blogs.gentoo.org/ago/2017/05/20/autotrace-multiple-vulnerabilities-the-autotrace-nightmare/	A-AUT-AUTOT-230617/72
NA	23-05-2017	7.5	libautotrace.a in AutoTrace 0.31.1 has a "cannot be represented in type int" issue in input-tga.c:192:19. **CVE ID: CVE-2017-9199**	https://blogs.gentoo.org/ago/2017/05/20/autotrace-multiple-vulnerabilities-the-autotrace-nightmare/	A-AUT-AUTOT-230617/73
NA	23-05-2017	7.5	libautotrace.a in AutoTrace 0.31.1 has a "cannot be represented in type int" issue in input-tga.c:508:18. **CVE ID: CVE-2017-9198**	https://blogs.gentoo.org/ago/2017/05/20/autotrace-multiple-vulnerabilities-the-autotrace-nightmare/	A-AUT-AUTOT-230617/74
NA	23-05-2017	7.5	libautotrace.a in AutoTrace 0.31.1 has a "cannot be represented in type int" issue in input-tga.c:498:55. **CVE ID: CVE-2017-9197**	https://blogs.gentoo.org/ago/2017/05/20/autotrace-multiple-vulnerabilities-the-autotrace-nightmare/	A-AUT-AUTOT-230617/75

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

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

NA	23-05-2017	7.5	libautotrace.a in AutoTrace 0.31.1 has a "negative-size-param" issue in the ReadImage function in input-tga.c:528:7. **CVE ID: CVE-2017-9196**	https://blogs.gentoo.org/ago/2017/05/20/autotrace-multiple-vulnerabilities-the-autotrace-nightmare/	A-AUT-AUTOT-230617/76
Overflow	23-05-2017	7.5	libautotrace.a in AutoTrace 0.31.1 has a heap-based buffer over-read in the ReadImage function in input-tga.c:620:27. **CVE ID: CVE-2017-9195**	https://blogs.gentoo.org/ago/2017/05/20/autotrace-multiple-vulnerabilities-the-autotrace-nightmare/	A-AUT-AUTOT-230617/77
Overflow	23-05-2017	7.5	libautotrace.a in AutoTrace 0.31.1 has a heap-based buffer over-read in the ReadImage function in input-tga.c:559:29. **CVE ID: CVE-2017-9194**	https://blogs.gentoo.org/ago/2017/05/20/autotrace-multiple-vulnerabilities-the-autotrace-nightmare/	A-AUT-AUTOT-230617/78
Overflow	23-05-2017	7.5	libautotrace.a in AutoTrace 0.31.1 has a heap-based buffer over-read in the ReadImage function in input-tga.c:538:33. **CVE ID: CVE-2017-9193**	https://blogs.gentoo.org/ago/2017/05/20/autotrace-multiple-vulnerabilities-the-autotrace-nightmare/	A-AUT-AUTOT-230617/79
Overflow	23-05-2017	7.5	libautotrace.a in AutoTrace 0.31.1 has a heap-based buffer overflow in the ReadImage function in input-tga.c:528:7. **CVE ID: CVE-2017-9192**	https://blogs.gentoo.org/ago/2017/05/20/autotrace-multiple-vulnerabilities-the-autotrace-nightmare/	A-AUT-AUTOT-230617/80
Overflow	23-05-2017	7.5	libautotrace.a in AutoTrace 0.31.1 has a heap-based buffer overflow in the rle_fread function in input-tga.c:252:15.	https://blogs.gentoo.org/ago/2017/05/20/autotrace-	A-AUT-AUTOT-230617/81

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

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

			CVE ID: CVE-2017-9191	multiple-vulnerabilities-the-autotrace-nightmare/	
NA	23-05-2017	7.5	libautotrace.a in AutoTrace 0.31.1 has a "left shift ... cannot be represented in type int" issue in input-bmp.c:516:63. **CVE ID: CVE-2017-9188**	https://blogs.gentoo.org/ago/2017/05/20/autotrace-multiple-vulnerabilities-the-autotrace-nightmare/	A-AUT-AUTOT-230617/82
NA	23-05-2017	7.5	libautotrace.a in AutoTrace 0.31.1 has a "cannot be represented in type int" issue in input-bmp.c:486:7. **CVE ID: CVE-2017-9187**	https://blogs.gentoo.org/ago/2017/05/20/autotrace-multiple-vulnerabilities-the-autotrace-nightmare/	A-AUT-AUTOT-230617/83
NA	23-05-2017	7.5	libautotrace.a in AutoTrace 0.31.1 has a "cannot be represented in type int" issue in input-bmp.c:326:17. **CVE ID: CVE-2017-9186**	https://blogs.gentoo.org/ago/2017/05/20/autotrace-multiple-vulnerabilities-the-autotrace-nightmare/	A-AUT-AUTOT-230617/84
NA	23-05-2017	7.5	libautotrace.a in AutoTrace 0.31.1 has a "cannot be represented in type int" issue in input-bmp.c:319:7. **CVE ID: CVE-2017-9185**	https://blogs.gentoo.org/ago/2017/05/20/autotrace-multiple-vulnerabilities-the-autotrace-nightmare/	A-AUT-AUTOT-230617/85
NA	23-05-2017	7.5	libautotrace.a in AutoTrace 0.31.1 has a "cannot be represented in type int" issue in input-bmp.c:314:7. **CVE ID: CVE-2017-9184**	https://blogs.gentoo.org/ago/2017/05/20/autotrace-multiple-vulnerabilities-the-autotrace-nightmare/	A-AUT-AUTOT-230617/86

NA	23-05-2017	7.5	libautotrace.a in AutoTrace 0.31.1 has a "cannot be represented in type int" issue in input-bmp.c:309:7. **CVE ID: CVE-2017-9183**	https://blogs.gentoo.org/ago/2017/05/20/autotrace-multiple-vulnerabilities-the-autotrace-nightmare/	A-AUT-AUTOT-230617/87
Overflow	23-05-2017	7.5	libautotrace.a in AutoTrace 0.31.1 has a heap-based buffer overflow in the ReadImage function in input-bmp.c:497:29. **CVE ID: CVE-2017-9173**	https://blogs.gentoo.org/ago/2017/05/20/autotrace-multiple-vulnerabilities-the-autotrace-nightmare/	A-AUT-AUTOT-230617/88
Overflow	23-05-2017	7.5	libautotrace.a in AutoTrace 0.31.1 has a heap-based buffer overflow in the ReadImage function in input-bmp.c:496:29. **CVE ID: CVE-2017-9172**	https://blogs.gentoo.org/ago/2017/05/20/autotrace-multiple-vulnerabilities-the-autotrace-nightmare/	A-AUT-AUTOT-230617/89
Overflow	23-05-2017	7.5	libautotrace.a in AutoTrace 0.31.1 has a heap-based buffer over-read in the ReadImage function in input-bmp.c:492:24. **CVE ID: CVE-2017-9171**	https://blogs.gentoo.org/ago/2017/05/20/autotrace-multiple-vulnerabilities-the-autotrace-nightmare/	A-AUT-AUTOT-230617/90
Overflow	23-05-2017	7.5	libautotrace.a in AutoTrace 0.31.1 has a heap-based buffer overflow in the ReadImage function in input-bmp.c:370:25. **CVE ID: CVE-2017-9170**	https://blogs.gentoo.org/ago/2017/05/20/autotrace-multiple-vulnerabilities-the-autotrace-nightmare/	A-AUT-AUTOT-230617/91
Overflow	23-05-2017	7.5	libautotrace.a in AutoTrace 0.31.1 has a heap-based buffer overflow in the ReadImage function in input-bmp.c:355:25.	https://blogs.gentoo.org/ago/2017/05/20/autotrace-	A-AUT-AUTOT-230617/92

			CVE ID: CVE-2017-9169	multiple-vulnerabilities-the-autotrace-nightmare/	
Overflow	23-05-2017	7.5	libautotrace.a in AutoTrace 0.31.1 has a heap-based buffer overflow in the ReadImage function in input-bmp.c:353:25. **CVE ID: CVE-2017-9168**	https://blogs.gentoo.org/ago/2017/05/20/autotrace-multiple-vulnerabilities-the-autotrace-nightmare/	A-AUT-AUTOT-230617/93
Overflow	23-05-2017	7.5	libautotrace.a in AutoTrace 0.31.1 has a heap-based buffer overflow in the ReadImage function in input-bmp.c:337:25. **CVE ID: CVE-2017-9167**	https://blogs.gentoo.org/ago/2017/05/20/autotrace-multiple-vulnerabilities-the-autotrace-nightmare/	A-AUT-AUTOT-230617/94
Overflow	23-05-2017	7.5	libautotrace.a in AutoTrace 0.31.1 has a heap-based buffer over-read in the GET_COLOR function in color.c:18:11. **CVE ID: CVE-2017-9166**	https://blogs.gentoo.org/ago/2017/05/20/autotrace-multiple-vulnerabilities-the-autotrace-nightmare/	A-AUT-AUTOT-230617/95
Overflow	23-05-2017	7.5	libautotrace.a in AutoTrace 0.31.1 has a heap-based buffer over-read in the GET_COLOR function in color.c:17:11. **CVE ID: CVE-2017-9165**	https://blogs.gentoo.org/ago/2017/05/20/autotrace-multiple-vulnerabilities-the-autotrace-nightmare/	A-AUT-AUTOT-230617/96
Overflow	23-05-2017	7.5	libautotrace.a in AutoTrace 0.31.1 has a heap-based buffer over-read in the GET_COLOR function in color.c:16:11. **CVE ID: CVE-2017-9164**	https://blogs.gentoo.org/ago/2017/05/20/autotrace-multiple-vulnerabilities-the-autotrace-nightmare/	A-AUT-AUTOT-230617/97

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

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

Overflow	23-05-2017	7.5	libautotrace.a in AutoTrace 0.31.1 has a "cannot be represented in type int" issue in pxl-outline.c:106:54. **CVE ID: CVE-2017-9163**	https://blogs.gentoo.org/ago/2017/05/20/autotrace-multiple-vulnerabilities-the-autotrace-nightmare/	A-AUT-AUTOT-230617/98
NA	23-05-2017	7.5	libautotrace.a in AutoTrace 0.31.1 has a "cannot be represented in type int" issue in autotrace.c:191:2. **CVE ID: CVE-2017-9162**	https://blogs.gentoo.org/ago/2017/05/20/autotrace-multiple-vulnerabilities-the-autotrace-nightmare/	A-AUT-AUTOT-230617/99
NA	23-05-2017	7.5	libautotrace.a in AutoTrace 0.31.1 has a "cannot be represented in type int" issue in autotrace.c:188:23. **CVE ID: CVE-2017-9161**	https://blogs.gentoo.org/ago/2017/05/20/autotrace-multiple-vulnerabilities-the-autotrace-nightmare/	A-AUT-AUTOT-230617/100
Overflow	23-05-2017	7.5	libautotrace.a in AutoTrace 0.31.1 has a stack-based buffer overflow in the pnmscanner_gettoken function in input-pnm.c:458:12. **CVE ID: CVE-2017-9160**	https://blogs.gentoo.org/ago/2017/05/20/autotrace-multiple-vulnerabilities-the-autotrace-nightmare/	A-AUT-AUTOT-230617/101
Overflow	23-05-2017	7.5	libautotrace.a in AutoTrace 0.31.1 has a heap-based buffer overflow in the pnm_load_rawpbm function in input-pnm.c:391:13. **CVE ID: CVE-2017-9153**	https://blogs.gentoo.org/ago/2017/05/20/autotrace-multiple-vulnerabilities-the-autotrace-nightmare/	A-AUT-AUTOT-230617/102
Overflow	23-05-2017	7.5	libautotrace.a in AutoTrace 0.31.1 has a heap-based buffer over-read in the pnm_load_raw function in input-pnm.c:346:41.	https://blogs.gentoo.org/ago/2017/05/20/autotrace-	A-AUT-AUTOT-230617/103

			CVE ID: CVE-2017-9152	multiple-vulnerabilities-the-autotrace-nightmare/	
Overflow	23-05-2017	7.5	libautotrace.a in AutoTrace 0.31.1 has a heap-based buffer overflow in the pnm_load_ascii function in input-pnm.c:303:12. **CVE ID: CVE-2017-9151**	https://blogs.gentoo.org/ago/2017/05/20/autotrace-multiple-vulnerabilities-the-autotrace-nightmare/	A-AUT-AUTOT-230617/104
Basercms					
Basercms					
CSRF	12-05-2017	6.8	Cross-site request forgery (CSRF) vulnerability in baserCMS plugin Uploader version 3.0.10 and earlier allows remote attackers to hijack the authentication of administrators via unspecified vectors. **CVE ID: CVE-2016-4887**	http://basercms.net/security/JVN92765814	A-BAS-BASER-230617/105
CSRF	12-05-2017	6.8	Cross-site request forgery (CSRF) vulnerability in baserCMS plugin Mail version 3.0.10 and earlier allows remote attackers to hijack the authentication of administrators via unspecified vectors. **CVE ID: CVE-2016-4886**	http://basercms.net/security/JVN92765814	A-BAS-BASER-230617/106
CSRF	12-05-2017	6.8	Cross-site request forgery (CSRF) vulnerability in baserCMS plugin Feed version 3.0.10 and earlier allows remote attackers to hijack the authentication of administrators via unspecified vectors. **CVE ID: CVE-2016-4885**	http://basercms.net/security/JVN92765814	A-BAS-BASER-230617/107
CSRF	12-05-2017	6.8	Cross-site request forgery (CSRF) vulnerability in baserCMS plugin Blog version 3.0.10 and earlier allows remote attackers to hijack the authentication of administrators via unspecified vectors. **CVE ID: CVE-2016-4884**	http://basercms.net/security/JVN92765814	A-BAS-BASER-230617/108
CSRF	12-05-2017	6.8	Cross-site request forgery (CSRF)	http://baserc	A-BAS-

			vulnerability in baserCMS version 3.0.10 and earlier allows remote attackers to hijack the authentication of administrators via unspecified vectors. **CVE ID: CVE-2016-4882**	ms.net/security/JVN92765814	BASER-230617/109
CSRF	12-05-2017	6.8	Cross-site request forgery (CSRF) vulnerability in baserCMS plugin Blog version 3.0.10 and earlier allows remote attackers to hijack the authentication of administrators via unspecified vectors. **CVE ID: CVE-2016-4881**	http://basercms.net/security/JVN92765814	A-BAS-BASER-230617/110
CSRF	12-05-2017	6.8	Cross-site request forgery (CSRF) vulnerability in baserCMS version 3.0.10 and earlier allows remote attackers to hijack the authentication of administrators via unspecified vectors. **CVE ID: CVE-2016-4878**	http://basercms.net/security/JVN92765814	A-BAS-BASER-230617/111
Execute Code CSRF	12-05-2017	6.8	Cross-site request forgery (CSRF) vulnerability in baserCMS version 3.0.10 and earlier allows remote attackers to hijack the authentication of administrators to execute arbitrary PHP code via unspecified vectors. **CVE ID: CVE-2016-4876**		A-BAS-BASER-230617/112
Basercms;Mail View					
CSRF	12-05-2017	6.8	Cross-site request forgery (CSRF) vulnerability in baserCMS plugin Mail version 3.0.10 and earlier allows remote attackers to hijack the authentication of administrators via unspecified vectors. **CVE ID: CVE-2016-4879**	http://basercms.net/security/JVN92765814	A-BAS-BASER-230617/113
Bitcoin					
Bitcoin					
NA	24-05-2017	5	The Bitcoin Proof-of-Work algorithm does not consider a certain attack methodology related to 80-byte block headers with a variety of initial 64-byte chunks followed by the same	NA	A-BIT-BITCO-230617/114

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

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

			16-byte chunk, multiple candidate root values ending with the same 4 bytes, and calculations involving sqrt numbers. This violates the security assumptions of (1) the choice of input, outside of the dedicated nonce area, fed into the Proof-of-Work function should not change its difficulty to evaluate and (2) every Proof-of-Work function execution should be independent. **CVE ID: CVE-2017-9230**		
Blackberry					
Enterprise Service;Unified Endpoint Manager					
XSS	10-05-2017	4.3	A stored cross site scripting vulnerability in the Management Console of BlackBerry Unified Endpoint Manager version 12.6.1 and earlier, and all versions of BES12, allows attackers to execute actions in the context of a Management Console administrator by uploading a malicious script and then persuading a target administrator to view the specific location of the malicious script within the Management Console. **CVE ID: CVE-2017-3894**	http://support.blackberry.com/kb/articleDetail?language=en_US&articleNumber=000044565	A-BLA-ENTER-230617/115
Cisco					
Firepower Threat Defense					
DoS	03-05-2017	5.5	A "Cisco Firepower Threat Defense 6.0.0 through 6.2.2 and Cisco ASA with FirePOWER Module Denial of Service" vulnerability in the access control policy of Cisco Firepower System Software could allow an authenticated, remote attacker to cause an affected system to stop inspecting and processing packets, resulting in a denial of service (DoS) condition. The vulnerability is due to improper SSL policy handling by the affected software when packets are	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170503-ftd	A-CIS-FIREP-230617/116

			passed through the sensing interfaces of an affected system. An attacker could exploit this vulnerability by sending crafted packets through a targeted system. This vulnerability affects Cisco Firepower System Software that is configured with the SSL policy feature. Cisco Bug IDs: CSCvc84361. **CVE ID: CVE-2017-6625**		
DoS	21-05-2017	7.8	A vulnerability in the logging configuration of Secure Sockets Layer (SSL) policies for Cisco FirePOWER System Software 5.3.0 through 6.2.2 could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition due to high consumption of system resources. The vulnerability is due to the logging of certain TCP packets by the affected software. An attacker could exploit this vulnerability by sending a flood of crafted TCP packets to an affected device. A successful exploit could allow the attacker to cause a DoS condition. The success of an exploit is dependent on how an administrator has configured logging for SSL policies for a device. This vulnerability affects Cisco FirePOWER System Software that is configured to log connections by using SSL policy default actions. Cisco Bug IDs: CSCvd07072. **CVE ID: CVE-2017-6632**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170517-fpwr	A-CIS-FIREP-230617/117
Identity Services Engine					
DoS	21-05-2017	5	A vulnerability in the TCP throttling process for the GUI of the Cisco Identity Services Engine (ISE) 2.1(0.474) could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170517-ise	A-CIS-IDENT-230617/118

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

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

			where the ISE GUI may fail to respond to new or established connection requests. The vulnerability is due to insufficient TCP rate limiting protection on the GUI. An attacker could exploit this vulnerability by sending the affected device a high rate of TCP connections to the GUI. An exploit could allow the attacker to cause the GUI to stop responding while the high rate of connections is in progress. Cisco Bug IDs: CSCvc81803. **CVE ID: CVE-2017-6653**		
Policy Suite					
Execute Code	18-05-2017	7.2	A vulnerability in a script file that is installed as part of the Cisco Policy Suite (CPS) Software distribution for the CPS appliance could allow an authenticated, local attacker to escalate their privilege level to root. The vulnerability is due to incorrect sudoers permissions on the script file. An attacker could exploit this vulnerability by authenticating to the device and providing crafted user input at the CLI, using this script file to escalate their privilege level and execute commands as root. A successful exploit could allow the attacker to acquire root-level privileges and take full control of the appliance. The user has to be logged-in to the device with valid credentials for a specific set of users. The Cisco Policy Suite application is vulnerable when running software versions 10.0.0, 10.1.0, or 11.0.0. Cisco Bug IDs: CSCvc07366. **CVE ID: CVE-2017-6623**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170517-cps	A-CIS-POLIC-230617/119
Prime Collaboration Provisioning					
Directory Traversal	21-05-2017	4	A vulnerability in the web interface of Cisco Prime Collaboration	https://tools.cisco.com/secur	A-CIS-PRIME-

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

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

			Provisioning Software (prior to Release 11.1) could allow an authenticated, remote attacker to delete any file from an affected system. The vulnerability exists because the affected software does not perform proper input validation of HTTP requests and fails to apply role-based access controls (RBACs) to requested HTTP URLs. An attacker could exploit this vulnerability by sending a crafted HTTP request that uses directory traversal techniques to submit a path to a desired file location on an affected system. A successful exploit could allow the attacker to delete any file from the system. Cisco Bug IDs: CSCvc99618. **CVE ID: CVE-2017-6637**	ity/center/content/CiscoSecurityAdvisory/cisco-sa-20170517-pcp5	230617/120
Directory Traversal	21-05-2017	4	A vulnerability in the web interface of Cisco Prime Collaboration Provisioning Software (prior to Release 11.1) could allow an authenticated, remote attacker to view any file on an affected system. The vulnerability exists because the affected software does not perform proper input validation of HTTP requests and fails to apply role-based access controls (RBACs) to requested HTTP URLs. An attacker could exploit this vulnerability by sending a crafted HTTP request that uses directory traversal techniques to submit a path to a desired file location on an affected system. A successful exploit could allow the attacker to view any file on the system. Cisco Bug IDs: CSCvc99604. **CVE ID: CVE-2017-6636**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170517-pcp4	A-CIS-PRIME-230617/121
Gain Information	18-05-2017	5	A vulnerability in the web interface of Cisco Prime Collaboration Provisioning could allow an unauthenticated, remote attacker to	https://tools.cisco.com/security/center/content/CiscoSecu	A-CIS-PRIME-230617/122

			access sensitive data. The attacker could use this information to conduct additional reconnaissance attacks. The vulnerability is due to insufficient protection of sensitive data when responding to an HTTP request on the web interface. An attacker could exploit the vulnerability by sending a crafted HTTP request to the application to access specific system files. An exploit could allow the attacker to obtain sensitive information about the application which could include user credentials. This vulnerability affects Cisco Prime Collaboration Provisioning Software Releases 10.6 through 11.5. Cisco Bug IDs: CSCvc99626. **CVE ID: CVE-2017-6621**	rityAdvisory/cisco-sa-20170517-pcp2	
Directory Traversal	21-05-2017	6.8	A vulnerability in the web interface of Cisco Prime Collaboration Provisioning Software (prior to Release 12.1) could allow an authenticated, remote attacker to delete any file from an affected system. The vulnerability exists because the affected software does not perform proper input validation of HTTP requests and fails to apply role-based access controls (RBACs) to requested HTTP URLs. An attacker could exploit this vulnerability by sending a crafted HTTP request that uses directory traversal techniques to submit a path to a desired file location on an affected system. A successful exploit could allow the attacker to delete any file from the system. Cisco Bug IDs: CSCvc99597. **CVE ID: CVE-2017-6635**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170517-pcp3	A-CIS-PRIME-230617/123
Bypass	18-05-2017	10	A vulnerability in the web interface for Cisco Prime Collaboration Provisioning could allow an	https://tools.cisco.com/security/center/con	A-CIS-PRIME-230617

			unauthenticated, remote attacker to bypass authentication and perform command injection with root privileges. The vulnerability is due to missing security constraints in certain HTTP request methods, which could allow access to files via the web interface. An attacker could exploit this vulnerability by sending a crafted HTTP request to the targeted application. This vulnerability affects Cisco Prime Collaboration Provisioning Software Releases prior to 12.1. Cisco Bug IDs: CSCvc98724. **CVE ID: CVE-2017-6622**	tent/CiscoSecurityAdvisory/cisco-sa-20170517-pcp1	/124
F5					
Big-ip Access Policy Manager					
XSS	09-05-2017	4.3	In F5 BIG-IP APM 12.0.0 through 12.1.2, non-authenticated users may be able to inject JavaScript into a request that will then be rendered and executed in the context of the Administrative user when the Administrative user is viewing the Access System Logs, allowing the non-authenticated user to carry out a Cross Site Scripting (XSS) attack against the Administrative user. **CVE ID: CVE-2016-9257**	https://support.f5.com/csp/article/K43523962	A-F5-BIG-I-230617/125
NA	09-05-2017	4.3	In F5 BIG-IP LTM, AAM, AFM, Analytics, APM, ASM, DNS, Edge Gateway, GTM, Link Controller, PEM, PSM, WebAccelerator, and WebSafe 11.6.1 HF1, 12.0.0 HF3, 12.0.0 HF4, and 12.1.0 through 12.1.2, undisclosed traffic patterns received while software SYN cookie protection is engaged may cause a disruption of service to the Traffic Management Microkernel (TMM) on specific platforms and configurations.	https://support.f5.com/csp/article/K82851041	A-F5-BIG-I-230617/126

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

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

			CVE ID: CVE-2017-6137		
NA	09-05-2017	5	In F5 BIG-IP 12.1.0 through 12.1.2, specific websocket traffic patterns may cause a disruption of service for virtual servers configured to use the websocket profile. **CVE ID: CVE-2016-9253**	https://support.f5.com/csp/article/K51351360	A-F5-BIG-I-230617/127
NA	09-05-2017	6	In F5 BIG-IP 12.1.0 through 12.1.2, permissions enforced by iControl can lag behind the actual permissions assigned to a user if the role_map is not reloaded between the time the permissions are changed and the time of the user's next request. This is a race condition that occurs rarely in normal usage; the typical period in which this is possible is limited to at most a few seconds after the permission change. **CVE ID: CVE-2016-9256**	https://support.f5.com/csp/article/K47284724	A-F5-BIG-I-230617/128
NA	09-05-2017	6.5	In F5 BIG-IP 12.0.0 through 12.1.2, an authenticated attacker may be able to cause an escalation of privileges through a crafted iControl REST connection. **CVE ID: CVE-2016-9251**	https://support.f5.com/csp/article/K41107914	A-F5-BIG-I-230617/129
NA	23-05-2017	7.5	In some circumstances, an F5 BIG-IP version 12.0.0 to 12.1.2 and 13.0.0 Azure cloud instance may contain a default administrative password which could be used to remotely log into the BIG-IP system. The impacted administrative account is the Azure instance administrative user that was created at deployment. The root and admin accounts are not vulnerable. An attacker may be able to remotely access the BIG-IP host via SSH. **CVE ID: CVE-2017-6131**	https://support.f5.com/csp/article/K61757346	A-F5-BIG-I-230617/130
Qemu					
Qemu					
NA	17-05-2017	4.6	Quick Emulator (Qemu) built with	https://bugzill	A-QEM-

			the VirtFS, host directory sharing via Plan 9 File System(9pfs) support, is vulnerable to an improper access control issue. It could occur while accessing virtfs metadata files in mapped-file security mode. A guest user could use this flaw to escalate their privileges inside guest. **CVE ID: CVE-2017-7493**	a.redhat.com/show_bug.cgi?id=1451709	QEMU-230617/131
DoS	23-05-2017	4.9	Memory leak in the keyboard input event handlers support in QEMU (aka Quick Emulator) allows local guest OS privileged users to cause a denial of service (host memory consumption) by rapidly generating large keyboard events. **CVE ID: CVE-2017-8379**		A-QEM-QEMU-230617/132
DoS	02-05-2017	4.9	hw/scsi/vmw_pvscsi.c in QEMU (aka Quick Emulator) allows local guest OS privileged users to cause a denial of service (infinite loop and CPU consumption) via the message ring page count. **CVE ID: CVE-2017-8112**	https://bugzilla.redhat.com/show_bug.cgi?id=1445621	A-QEM-QEMU-230617/133
DoS	02-05-2017	4.9	Memory leak in the v9fs_list_xattr function in hw/9pfs/9p-xattr.c in QEMU (aka Quick Emulator) allows local guest OS privileged users to cause a denial of service (memory consumption) via vectors involving the orig_value variable. **CVE ID: CVE-2017-8086**	https://bugzilla.redhat.com/show_bug.cgi?id=1444781	A-QEM-QEMU-230617/134
DoS	23-05-2017	7.8	Memory leak in the audio/audio.c in QEMU (aka Quick Emulator) allows remote attackers to cause a denial of service (memory consumption) by repeatedly starting and stopping audio capture. **CVE ID: CVE-2017-8309**		A-QEM-QEMU-230617/135
SAP					
Business One					
NA	25-05-2017	6.8	SAP Business One for Android 1.2.3 allows remote attackers to conduct	NA	A-SAP-BUSIN-

			XML External Entity (XXE) attacks via crafted XML data in a request to B1iXcellerator/exec/soap/vP.001sap0003.in_WCSX/com.sap.b1i.vplatform.runtime/INB_WS_CALL_SYNC_XPT/INB_WS_CALL_SYNC_XPT.ipo/proc, aka SAP Security Note 2378065. **CVE ID: CVE-2016-6256**		230617/136
Hana Xs					
DoS	23-05-2017	5	sinopia, as used in SAP HANA XS 1.00 and 2.00, allows remote attackers to cause a denial of service (assertion failure and service crash) by pushing a package with a filename containing a $ (dollar sign) or % (percent) character, aka SAP Security Note 2407694. **CVE ID: CVE-2017-8915**	NA	A-SAP-HANA - 230617/137
NA	23-05-2017	7.5	sinopia, as used in SAP HANA XS 1.00 and 2.00, allows remote attackers to hijack npm packages or host arbitrary files by leveraging an insecure user creation policy, aka SAP Security Note 2407694. **CVE ID: CVE-2017-8914**	NA	A-SAP-HANA - 230617/138
Netweaver					
NA	23-05-2017	6.5	The Visual Composer VC70RUNTIME component in SAP NetWeaver AS JAVA 7.5 allows remote authenticated users to conduct XML External Entity (XXE) attacks via a crafted XML document in a request to irj/servlet/prt/portal/prtroot/com.sap.visualcomposer.BIKit.default, aka SAP Security Note 2386873. **CVE ID: CVE-2017-8913**	NA	A-SAP-NETWE-230617/139
Sapcar					
Overflow	10-05-2017	6.8	SAP SAPCAR 721.510 has a Heap Based Buffer Overflow Vulnerability. It could be exploited with a crafted CAR archive file received from an untrusted remote source. The	NA	A-SAP-SAPCA-230617/140

			problem is that the length of data written is an arbitrary number found within the file. The vendor response is SAP Security Note 2441560. **CVE ID: CVE-2017-8852**		
Trendmicro					
Officescan					
Gain Privileges	03-05-2017	4	Trend Micro OfficeScan 11.0 before SP1 CP 6325 and XG before CP 1352 allows remote authenticated users to gain privileges by leveraging a leak of an encrypted password during a web-console operation. **CVE ID: CVE-2017-5481**	https://success.trendmicro.com/solution/1117204	A-TRE-OFFIC-230617/141
XSS	05-05-2017	4.3	Trend Micro OfficeScan 11.0 before SP1 CP 6325 (with Agent Module Build before 6152) and XG before CP 1352 has XSS via a crafted URI using a blocked website. **CVE ID: CVE-2017-8801**	https://success.trendmicro.com/solution/1117204-security-bulletin-trend-micro-officescan-11-xg-multiple-vulnerabilities	A-TRE-OFFIC-230617/142
Serverprotect					
XSS	25-05-2017	4.3	Multiple cross-site scripting (XSS) vulnerabilities in Trend Micro ServerProtect for Linux 3.0 before CP 1531 allow remote attackers to inject arbitrary web script or HTML via the (1) S44, (2) S5, (3) S_action_fail, (4) S_ptn_update, (5) T113, (6) T114, (7) T115, (8) T117117, (9) T118, (10) T_action_fail, (11) T_ptn_update, (12) textarea, (13) textfield5, or (14) tmLastConfigFileModifiedDate parameter to notification.cgi. **CVE ID: CVE-2017-9037**	https://success.trendmicro.com/solution/1117411	A-TRE-SERVE-230617/143
XSS	25-05-2017	4.3	Multiple cross-site scripting (XSS) vulnerabilities in Trend Micro ServerProtect for Linux 3.0 before CP 1531 allow remote attackers to inject arbitrary web script or HTML via the	https://success.trendmicro.com/solution/1117411	A-TRE-SERVE-230617/144

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

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

			(1) T1 or (2) tmLastConfigFileModifiedDate parameter to log_management.cgi. **CVE ID: CVE-2017-9032**		
Gain Information	25-05-2017	5.8	Trend Micro ServerProtect for Linux 3.0 before CP 1531 allows attackers to eavesdrop and tamper with updates by leveraging unencrypted communications with update servers. **CVE ID: CVE-2017-9035**	https://success.trendmicro.com/solution/1117411	A-TRE-SERVE-230617/145
CSRF	25-05-2017	6.8	Cross-site request forgery (CSRF) vulnerability in Trend Micro ServerProtect for Linux 3.0 before CP 1531 allows remote attackers to hijack the authentication of users for requests to start an update from an arbitrary source via a crafted request to SProtectLinux/scanoption_set.cgi, related to the lack of anti-CSRF tokens. **CVE ID: CVE-2017-9033**	https://success.trendmicro.com/solution/1117411	A-TRE-SERVE-230617/146
Gain Privileges	25-05-2017	7.2	Trend Micro ServerProtect for Linux 3.0 before CP 1531 allows local users to gain privileges by leveraging an unrestricted quarantine directory. **CVE ID: CVE-2017-9036**	https://success.trendmicro.com/solution/1117411	A-TRE-SERVE-230617/147
Execute Code	25-05-2017	10	Trend Micro ServerProtect for Linux 3.0 before CP 1531 allows attackers to write to arbitrary files and consequently execute arbitrary code with root privileges by leveraging failure to validate software updates. **CVE ID: CVE-2017-9034**	https://success.trendmicro.com/solution/1117411	A-TRE-SERVE-230617/148
Ytnef Project					
Ytnef					
DoS Overflow	22-05-2017	6.8	The TNEFFillMapi function in lib/ytnef.c in libytnef in ytnef through 1.9.2 does not ensure a nonzero count value before a certain memory allocation, which allows remote attackers to cause a denial of service (heap-based buffer overflow	NA	A-YTN-YTNEF-230617/149

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

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

			and application crash) or possibly have unspecified other impact via a crafted tnef file. **CVE ID: CVE-2017-9146**		
Overflow	18-05-2017	7.5	In libytnef in ytnef through 1.9.2, there is a heap-based buffer over-read due to incorrect boundary checking in the SIZECHECK macro in lib/ytnef.c. **CVE ID: CVE-2017-9058**	https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=862556	A-YTN-YTNEF-230617/150
Zimbra					
Zimbra Collaboration Suite					
XSS	23-05-2017	4.3	Cross-site scripting (XSS) vulnerability in Zimbra Collaboration Suite (ZCS) before 8.7.1 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors. **CVE ID: CVE-2017-7288**	https://wiki.zimbra.com/wiki/Zimbra_Security_Advisories	A-ZIM-ZIMBR-230617/151
CSRF	17-05-2017	6.8	Multiple cross-site request forgery (CSRF) vulnerabilities in the Admin Console in Zimbra Collaboration before 8.6.0 Patch 8 allow remote attackers to hijack the authentication of administrators for requests that (1) add, (2) modify, or (3) remove accounts by leveraging failure to use of a CSRF token and perform referer header checks, aka bugs 100885 and 100899. **CVE ID: CVE-2016-3403**	https://wiki.zimbra.com/wiki/Zimbra_Security_Advisories	A-ZIM-ZIMBR-230617/152
Directory Traversal	23-05-2017	7.5	Directory traversal vulnerability in Zimbra Collaboration Suite (aka ZCS) before 8.7.6 allows attackers to have unspecified impact via unknown vectors. **CVE ID: CVE-2017-6821**	https://wiki.zimbra.com/wiki/Security_Center	A-ZIM-ZIMBR-230617/153
NA	23-05-2017	7.5	A service provided by Zimbra Collaboration Suite (ZCS) before 8.7.6 fails to require needed privileges before performing a few requested operations. **CVE ID: CVE-2017-6813**	https://wiki.zimbra.com/wiki/Security_Center	A-ZIM-ZIMBR-230617/154

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

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

Application / Hardware					
F5/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 Edge Gateway;Big-ip Global Traffic Manager;Big-ip Link Controller;Big-ip Local Traffic Manager;Big-ip Policy Enforcement Manager;Big-ip Webaccelerator;Big-ip Websafe/Big-ip Protocol Security Manager					
NA	10-05-2017	5	In F5 BIG-IP 11.2.1, 11.4.0 through 11.6.1, and 12.0.0 through 12.1.2, an unauthenticated user with access to the control plane may be able to delete arbitrary files through an undisclosed mechanism. **CVE ID: CVE-2016-9250**	https://support.f5.com/csp/article/K55792317	A-H-F5-BIG-I-230617/155
NA	01-05-2017	5	An attacker may be able to cause a denial-of-service (DoS) attack against the sshd component in F5 BIG-IP, Enterprise Manager, BIG-IQ, and iWorkflow. **CVE ID: CVE-2017-6128**	https://support.f5.com/csp/article/K92140924	A-H-F5-BIG-I-230617/156
Big-ip Access Policy Manager;Big-ip Advanced Firewall Manager;Big-ip Application Acceleration Manager;Big-ip Application Security Manager;Big-ip Global Traffic Manager;Big-ip Link Controller;Big-ip Local Traffic Manager;Big-ip Policy Enforcement Manager;Big-ip Websafe/Big-ip Protocol Security Manager					
DoS	11-05-2017	5	The Traffic Management Microkernel (TMM) in F5 BIG-IP LTM, AAM, AFM, APM, ASM, GTM, Link Controller, PEM, PSM, and WebSafe 11.6.0 before 11.6.0 HF6, 11.5.0 before 11.5.3 HF2, and 11.3.0 before 11.4.1 HF10 may suffer from a memory leak while handling certain types of TCP traffic. Remote attackers may cause a denial of service (DoS) by way of a crafted TCP packet. **CVE ID: CVE-2016-7476**	https://support.f5.com/csp/#/article/K87416818	A-H-F5-BIG-I-230617/157
Application / OS					
Apple/Apple					
Apple Tv/Iphone Os;Mac Os X;Watchos					
Bypass; Gain Information	22-05-2017	4.3	An issue was discovered in certain Apple products. iOS before 10.3.2 is affected. macOS before 10.12.5 is	https://support.apple.com/HT207797	A-0S-APP-APPLE-

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

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

			affected. tvOS before 10.2.1 is affected. watchOS before 3.2.2 is affected. The issue involves the "Kernel" component. It allows attackers to bypass intended memory-read restrictions via a crafted app. **CVE ID: CVE-2017-6987**		230617/158
Bypass Gain Information	22-05-2017	4.3	An issue was discovered in certain Apple products. iOS before 10.3.2 is affected. macOS before 10.12.5 is affected. tvOS before 10.2.1 is affected. watchOS before 3.2.2 is affected. The issue involves the "Kernel" component. It allows attackers to bypass intended memory-read restrictions via a crafted app. **CVE ID: CVE-2017-2507**	https://support.apple.com/HT207801	A-OS-APP-APPLE-230617/159
Bypass	22-05-2017	4.3	An issue was discovered in certain Apple products. iOS before 10.3.2 is affected. macOS before 10.12.5 is affected. tvOS before 10.2.1 is affected. watchOS before 3.2.2 is affected. The issue involves the "CoreAudio" component. It allows attackers to bypass intended memory-read restrictions via a crafted app. **CVE ID: CVE-2017-2502**	https://support.apple.com/HT207801	A-OS-APP-APPLE-230617/160
DoS Execute Code Overflow Memory Corruption	22-05-2017	6.8	An issue was discovered in certain Apple products. iOS before 10.3.2 is affected. Safari before 10.1.1 is affected. tvOS before 10.2.1 is affected. watchOS before 3.2.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site. **CVE ID: CVE-2017-2521**	https://support.apple.com/HT207798	A-OS-APP-APPLE-230617/161
DoS Execute Code	22-05-2017	7.5	An issue was discovered in certain Apple products. iOS before 10.3.2 is	https://support.apple.com/	A-OS-APP-

Overflow Memory Corruption			affected. macOS before 10.12.5 is affected. tvOS before 10.2.1 is affected. watchOS before 3.2.2 is affected. The issue involves the "TextInput" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via crafted data. **CVE ID: CVE-2017-2524**	HT207797	APPLE-230617/162
DoS Execute Code Overflow Memory Corruption	22-05-2017	7.5	An issue was discovered in certain Apple products. iOS before 10.3.2 is affected. macOS before 10.12.5 is affected. tvOS before 10.2.1 is affected. watchOS before 3.2.2 is affected. The issue involves the "Foundation" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via crafted data. **CVE ID: CVE-2017-2523**	https://support.apple.com/HT207797	A-OS-APP-APPLE-230617/163
DoS Execute Code Overflow Memory Corruption	22-05-2017	7.5	An issue was discovered in certain Apple products. iOS before 10.3.2 is affected. macOS before 10.12.5 is affected. tvOS before 10.2.1 is affected. watchOS before 3.2.2 is affected. The issue involves the "CoreFoundation" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via crafted data. **CVE ID: CVE-2017-2522**	https://support.apple.com/HT207801	A-OS-APP-APPLE-230617/164
DoS Execute Code Overflow	22-05-2017	7.5	An issue was discovered in certain Apple products. iOS before 10.3.2 is affected. macOS before 10.12.5 is affected. tvOS before 10.2.1 is affected. watchOS before 3.2.2 is affected. The issue involves the "SQLite" component. It allows remote attackers to execute arbitrary code or cause a denial of service (buffer overflow and application	https://support.apple.com/HT207797	A-OS-APP-APPLE-230617/165

			crash) via a crafted SQL statement. **CVE ID: CVE-2017-2520**		
DoS Execute Code Overflow Memory Corruption	22-05-2017	7.5	An issue was discovered in certain Apple products. iOS before 10.3.2 is affected. macOS before 10.12.5 is affected. tvOS before 10.2.1 is affected. watchOS before 3.2.2 is affected. The issue involves the "SQLite" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted SQL statement. **CVE ID: CVE-2017-2519**	https://support.apple.com/HT207797	A-OS-APP-APPLE-230617/166
DoS Execute Code Overflow	22-05-2017	7.5	An issue was discovered in certain Apple products. iOS before 10.3.2 is affected. macOS before 10.12.5 is affected. tvOS before 10.2.1 is affected. watchOS before 3.2.2 is affected. The issue involves the "SQLite" component. It allows remote attackers to execute arbitrary code or cause a denial of service (buffer overflow and application crash) via a crafted SQL statement. **CVE ID: CVE-2017-2518**	https://support.apple.com/HT207801	A-OS-APP-APPLE-230617/167
DoS Execute Code	22-05-2017	7.5	An issue was discovered in certain Apple products. iOS before 10.3.2 is affected. macOS before 10.12.5 is affected. tvOS before 10.2.1 is affected. watchOS before 3.2.2 is affected. The issue involves the "SQLite" component. A use-after-free vulnerability allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via a crafted SQL statement. **CVE ID: CVE-2017-2513**	https://support.apple.com/HT207801	A-OS-APP-APPLE-230617/168
Execute Code	22-05-2017	7.6	An issue was discovered in certain Apple products. iOS before 10.3.2 is affected. macOS before 10.12.5 is affected. tvOS before 10.2.1 is affected. watchOS before 3.2.2 is affected. The issue involves the	https://support.apple.com/HT207801	A-OS-APP-APPLE-230617/169

			"IOSurface" component. A race condition allows attackers to execute arbitrary code in a privileged context via a crafted app. **CVE ID: CVE-2017-6979**		
Execute Code	22-05-2017	7.6	An issue was discovered in certain Apple products. iOS before 10.3.2 is affected. macOS before 10.12.5 is affected. tvOS before 10.2.1 is affected. watchOS before 3.2.2 is affected. The issue involves the "Kernel" component. A race condition allows attackers to execute arbitrary code in a privileged context via a crafted app. **CVE ID: CVE-2017-2501**	https://support.apple.com/HT207801	A-OS-APP-APPLE-230617/170
Apple Tv/Iphone Os;Safari;Watchos					
XSS	22-05-2017	4.3	An issue was discovered in certain Apple products. iOS before 10.3.2 is affected. Safari before 10.1.1 is affected. tvOS before 10.2.1 is affected. The issue involves the "WebKit" component. It allows remote attackers to conduct Universal XSS (UXSS) attacks via a crafted web site that improperly interacts with WebKit Editor commands. **CVE ID: CVE-2017-2504**	https://support.apple.com/HT207804	A-OS-APP-APPLE-230617/171
DoS Execute Code Overflow Memory Corruption	22-05-2017	6.8	An issue was discovered in certain Apple products. iOS before 10.3.2 is affected. Safari before 10.1.1 is affected. tvOS before 10.2.1 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site. **CVE ID: CVE-2017-2515**	https://support.apple.com/HT207804	A-OS-APP-APPLE-230617/172
DoS Execute Code Memory Corruption	22-05-2017	6.8	An issue was discovered in certain Apple products. iOS before 10.3.2 is affected. Safari before 10.1.1 is affected. tvOS before 10.2.1 is	https://support.apple.com/HT207804	A-OS-APP-APPLE-230617

			affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site. **CVE ID: CVE-2017-2505**		/173
DoS Execute Code Overflow Memory Corruption	22-05-2017	6.8	An issue was discovered in certain Apple products. iOS before 10.3.2 is affected. Safari before 10.1.1 is affected. tvOS before 10.2.1 is affected. The issue involves the "WebKit Web Inspector" component. It allows attackers to execute arbitrary unsigned code or cause a denial of service (memory corruption) via a crafted app. **CVE ID: CVE-2017-2499**	https://support.apple.com/HT207804	A-OS-APP-APPLE-230617/174
DoS Execute Code Overflow Memory Corruption	22-05-2017	9.3	An issue was discovered in certain Apple products. iOS before 10.3.2 is affected. tvOS before 10.2.1 is affected. watchOS before 3.2.2 is affected. The issue involves the "AVEVideoEncoder" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app. **CVE ID: CVE-2017-6999**	https://support.apple.com/HT207801	A-OS-APP-APPLE-230617/175
DoS Execute Code Overflow Memory Corruption	22-05-2017	9.3	An issue was discovered in certain Apple products. iOS before 10.3.2 is affected. tvOS before 10.2.1 is affected. watchOS before 3.2.2 is affected. The issue involves the "AVEVideoEncoder" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app. **CVE ID: CVE-2017-6998**	https://support.apple.com/HT207801	A-OS-APP-APPLE-230617/176
Iphone Os/Safari					
DoS Execute Code Overflow	22-05-2017	6.8	An issue was discovered in certain Apple products. iOS before 10.3.2 is affected. Safari before 10.1.1 is	https://support.apple.com/HT207804	A-OS-APP-IPHON-

Memory Corruption			affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site. **CVE ID: CVE-2017-2526**		230617/177
DoS Execute Code Overflow Memory Corruption	22-05-2017	6.8	An issue was discovered in certain Apple products. iOS before 10.3.2 is affected. Safari before 10.1.1 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site. **CVE ID: CVE-2017-2506**	https://support.apple.com/HT207804	A-OS-APP-IPHON-230617/178
GNU/Novell;Opensuse Project					
Zlib/Leap/Leap;Opensuse					
NA	23-05-2017	6.8	The inflateMark function in inflate.c in zlib 1.2.8 might allow context-dependent attackers to have unspecified impact via vectors involving left shifts of negative integers. **CVE ID: CVE-2016-9842**	https://bugzilla.redhat.com/show_bug.cgi?id=1402348	A-OS-GNU-ZLIB/-230617/179
NA	23-05-2017	6.8	inftrees.c in zlib 1.2.8 might allow context-dependent attackers to have unspecified impact by leveraging improper pointer arithmetic. **CVE ID: CVE-2016-9840**	https://bugzilla.redhat.com/show_bug.cgi?id=1402345	A-OS-GNU-ZLIB/-230617/180
NA	23-05-2017	7.5	The crc32_big function in crc32.c in zlib 1.2.8 might allow context-dependent attackers to have unspecified impact via vectors involving big-endian CRC calculation. **CVE ID: CVE-2016-9843**	https://bugzilla.redhat.com/show_bug.cgi?id=1402351	A-OS-GNU-ZLIB/-230617/181
NA	23-05-2017	7.5	inffast.c in zlib 1.2.8 might allow context-dependent attackers to have unspecified impact by leveraging improper pointer arithmetic. **CVE ID: CVE-2016-9841**	https://bugzilla.redhat.com/show_bug.cgi?id=1402346	A-OS-GNU-ZLIB/-230617/182

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

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

OS					
Apple					
Iphone Os					
DoS Overflow	22-05-2017	4.3	An issue was discovered in certain Apple products. iOS before 10.3.2 is affected. The issue involves the "Notifications" component. It allows attackers to cause a denial of service via a crafted app. **CVE ID: CVE-2017-6982**	https://support.apple.com/HT207798	O-APP-IPHON-230617/183
Bypass	22-05-2017	5	An issue was discovered in certain Apple products. iOS before 10.3.2 is affected. The issue involves the "Security" component. It allows attackers to bypass intended access restrictions via an untrusted certificate. **CVE ID: CVE-2017-2498**	https://support.apple.com/HT207798	O-APP-IPHON-230617/184
Iphone Os;Mac Os X					
	22-05-2017	5.8	An issue was discovered in certain Apple products. iOS before 10.3.2 is affected. macOS before 10.12.5 is affected. The issue involves the "iBooks" component. It allows remote attackers to trigger visits to arbitrary URLs via a crafted book. **CVE ID: CVE-2017-2497**	https://support.apple.com/HT207798	O-APP-IPHON-230617/185
DoS Execute Code Overflow Memory Corruption	22-05-2017	6.8	An issue was discovered in certain Apple products. iOS before 10.3.2 is affected. macOS before 10.12.5 is affected. The issue involves the "SQLite" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site. **CVE ID: CVE-2017-6991**	https://support.apple.com/HT207798	O-APP-IPHON-230617/186
DoS Execute Code Overflow Memory Corruption	22-05-2017	6.8	An issue was discovered in certain Apple products. iOS before 10.3.2 is affected. macOS before 10.12.5 is affected. The issue involves the "SQLite" component. It allows remote attackers to execute arbitrary	https://support.apple.com/HT207798	O-APP-IPHON-230617/187

			code or cause a denial of service (memory corruption and application crash) via a crafted web site. **CVE ID: CVE-2017-6983**		
Execute Code	22-05-2017	9.3	An issue was discovered in certain Apple products. iOS before 10.3.2 is affected. macOS before 10.12.5 is affected. The issue involves the "iBooks" component. It allows attackers to execute arbitrary code in a privileged context via a crafted app that uses symlinks. **CVE ID: CVE-2017-6981**	https://support.apple.com/HT207798	O-APP-IPHON-230617/188
Iphone Os;Safari					
DoS	22-05-2017	4.3	An issue was discovered in certain Apple products. iOS before 10.3.2 is affected. Safari before 10.1.1 is affected. The issue involves the "Safari" component. It allows remote attackers to cause a denial of service (application crash) via a crafted web site that improperly interacts with the history menu. **CVE ID: CVE-2017-2495**	https://support.apple.com/HT207804	O-APP-IPHON-230617/189
DoS Execute Code Overflow Memory Corruption	22-05-2017	6.8	An issue was discovered in certain Apple products. iOS before 10.3.2 is affected. Safari before 10.1.1 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site. **CVE ID: CVE-2017-2514**	https://support.apple.com/HT207804	O-APP-IPHON-230617/190
DoS Execute Code Overflow Memory Corruption	22-05-2017	6.8	An issue was discovered in certain Apple products. iOS before 10.3.2 is affected. Safari before 10.1.1 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site. **CVE ID: CVE-2017-2496**	https://support.apple.com/HT207804	O-APP-IPHON-230617/191

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

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

Mac Os X					
Bypass	22-05-2017	4.3	An issue was discovered in certain Apple products. macOS before 10.12.5 is affected. The issue involves the "HFS" component. It allows attackers to bypass intended memory-read restrictions via a crafted app. **CVE ID: CVE-2017-6990**	https://support.apple.com/HT207797	O-APP-MAC O-230617/192
NA	22-05-2017	4.3	An issue was discovered in certain Apple products. macOS before 10.12.5 is affected. The issue involves the "802.1X" component. It allows remote attackers to discover the network credentials of arbitrary users by operating a crafted network that requires 802.1X authentication, because EAP-TLS certificate validation mishandles certificate changes. **CVE ID: CVE-2017-6988**	https://support.apple.com/HT207797	O-APP-MAC O-230617/193
Bypass	22-05-2017	4.3	An issue was discovered in certain Apple products. macOS before 10.12.5 is affected. The issue involves the "WindowServer" component. It allows attackers to bypass intended memory-read restrictions via a crafted app. **CVE ID: CVE-2017-2540**	https://support.apple.com/HT207797	O-APP-MAC O-230617/194
Bypass	22-05-2017	4.3	An issue was discovered in certain Apple products. macOS before 10.12.5 is affected. The issue involves the "Kernel" component. It allows attackers to bypass intended memory-read restrictions via a crafted app. **CVE ID: CVE-2017-2516**	https://support.apple.com/HT207797	O-APP-MAC O-230617/195
Bypass	22-05-2017	4.3	An issue was discovered in certain Apple products. macOS before 10.12.5 is affected. The issue involves the "Kernel" component. It allows attackers to bypass intended memory-read restrictions via a crafted app.	https://support.apple.com/HT207797	O-APP-MAC O-230617/196

			CVE ID: CVE-2017-2509		
DoS Overflow Memory Corruption	22-05-2017	6.8	An issue was discovered in certain Apple products. macOS before 10.12.5 is affected. The issue involves the "iBooks" component. It allows attackers to conduct sandbox-escape attacks or cause a denial of service (memory corruption) via a crafted app. **CVE ID: CVE-2017-6986**	https://support.apple.com/HT207797	O-APP-MAC O-230617/197
DoS Overflow Memory Corruption	22-05-2017	6.8	An issue was discovered in certain Apple products. macOS before 10.12.5 is affected. The issue involves the "Speech Framework" component. It allows attackers to conduct sandbox-escape attacks or cause a denial of service (memory corruption) via a crafted app. **CVE ID: CVE-2017-6977**	https://support.apple.com/HT207797	O-APP-MAC O-230617/198
DoS	22-05-2017	6.8	An issue was discovered in certain Apple products. macOS before 10.12.5 is affected. The issue involves the "Security" component. It allows attackers to conduct sandbox-escape attacks or cause a denial of service (resource consumption) via a crafted app. **CVE ID: CVE-2017-2535**	https://support.apple.com/HT207797	O-APP-MAC O-230617/199
NA	22-05-2017	6.8	An issue was discovered in certain Apple products. macOS before 10.12.5 is affected. The issue involves the "Speech Framework" component. It allows attackers to conduct sandbox-escape attacks via a crafted app. **CVE ID: CVE-2017-2534**	https://support.apple.com/HT207797	O-APP-MAC O-230617/200
DoS Overflow Memory Corruption	22-05-2017	6.8	An issue was discovered in certain Apple products. macOS before 10.12.5 is affected. The issue involves the "Sandbox" component. It allows attackers to conduct sandbox-escape attacks or cause a denial of service (memory corruption) via a crafted app.	https://support.apple.com/HT207797	O-APP-MAC O-230617/201

			CVE ID: CVE-2017-2512		
DoS Execute Code Overflow	22-05-2017	7.5	An issue was discovered in certain Apple products. macOS before 10.12.5 is affected. The issue involves the "CoreAnimation" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory consumption and application crash) via crafted data. **CVE ID: CVE-2017-2527**	https://support.apple.com/HT207797	O-APP-MAC O-230617/202
Execute Code	22-05-2017	7.6	An issue was discovered in certain Apple products. macOS before 10.12.5 is affected. The issue involves the "DiskArbitration" component. A race condition allows attackers to execute arbitrary code in a privileged context via a crafted app. **CVE ID: CVE-2017-2533**	https://support.apple.com/HT207797	O-APP-MAC O-230617/203
DoS Execute Code Overflow Memory Corruption	22-05-2017	9.3	An issue was discovered in certain Apple products. macOS before 10.12.5 is affected. The issue involves the "NVIDIA Graphics Drivers" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app. **CVE ID: CVE-2017-6985**	https://support.apple.com/HT207797	O-APP-MAC O-230617/204
DoS Execute Code Overflow Memory Corruption	22-05-2017	9.3	An issue was discovered in certain Apple products. macOS before 10.12.5 is affected. The issue involves the "Accessibility Framework" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app. **CVE ID: CVE-2017-6978**	https://support.apple.com/HT207797	O-APP-MAC O-230617/205
DoS Execute Code Overflow Memory Corruption	22-05-2017	9.3	An issue was discovered in certain Apple products. macOS before 10.12.5 is affected. The issue involves the "WindowServer" component. It allows attackers to execute arbitrary code in a privileged context or cause	https://support.apple.com/HT207797	O-APP-MAC O-230617/206

			a denial of service (memory corruption) via a crafted app. **CVE ID: CVE-2017-2548**		
Safari					
	22-05-2017	4.3	An issue was discovered in certain Apple products. Safari before 10.1.1 is affected. The issue involves the "Safari" component. It allows remote attackers to spoof the address bar via a crafted web site. **CVE ID: CVE-2017-2500**	https://support.apple.com/HT207804	O-APP-SAFAR-230617/207
Geutebruck					
Ip Camera G-cam Efd-2250 Firmware					
Execute Code Bypass	18-05-2017	7.5	An Authentication Bypass issue was discovered in Geutebruck IP Camera G-Cam/EFD-2250 Version 1.11.0.12. An authentication bypass vulnerability has been identified. The existing file system architecture could allow attackers to bypass the access control that may allow remote code execution. **CVE ID: CVE-2017-5174**	NA	O-GEU-IP CA-230617/208
Execute Code	18-05-2017	10	An Improper Neutralization of Special Elements (in an OS command) issue was discovered in Geutebruck IP Camera G-Cam/EFD-2250 Version 1.11.0.12. An improper neutralization of special elements vulnerability has been identified. If special elements are not properly neutralized, an attacker can call multiple parameters that can allow access to the root level operating system which could allow remote code execution. **CVE ID: CVE-2017-5173**	NA	O-GEU-IP CA-230617/209
Google					
Android					
Gain Information	12-05-2017	4.3	An information disclosure vulnerability in the MediaTek command queue driver could enable a local malicious application to	https://source.android.com/security/bulletin/01-05-2017	O-GOO-ANDRO-230617/210

			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-35142799. References: M-ALPS03161531. **CVE ID: CVE-2017-0625**		
Bypass Gain Information	12-05-2017	4.3	An information disclosure vulnerability in Bluetooth could allow a local malicious application to bypass operating system protections that isolate application data from other applications. This issue is rated as Moderate due to details specific to the vulnerability. Product: Android. Versions: 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2. Android ID: A-34946955. **CVE ID: CVE-2017-0602**	https://source.android.com/security/bulletin/01-05-2017	O-GOO-ANDRO-230617/211
Bypass	12-05-2017	4.3	An Elevation of Privilege vulnerability in Bluetooth could potentially enable a local malicious application to accept harmful files shared via bluetooth without user permission. This issue is rated as Moderate due to local bypass of user interaction requirements. Product: Android. Versions: 7.0, 7.1.1, 7.1.2. Android ID: A-35258579. **CVE ID: CVE-2017-0601**	https://source.android.com/security/bulletin/01-05-2017	O-GOO-ANDRO-230617/212
Bypass Gain Information	12-05-2017	4.3	An information disclosure vulnerability in the Framework APIs could enable a local malicious application to bypass operating system protections that isolate application data from other applications. This issue is rated as High because it could be used to gain access to data that the application does not have access to. Product: Android. Versions: 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2. Android ID:	https://source.android.com/security/bulletin/01-05-2017	O-GOO-ANDRO-230617/213

			A-34128677. **CVE ID: CVE-2017-0598**		
Bypass Gain Information	12-05-2017	4.3	An information disclosure vulnerability in File-Based Encryption could enable a local malicious attacker to bypass operating system protections for the lock screen. This issue is rated as Moderate due to the possibility of bypassing the lock screen. Product: Android. Versions: 7.0, 7.1.1. Android ID: A-32793550. **CVE ID: CVE-2017-0493**	https://source.android.com/security/bulletin/01-05-2017	O-GOO-ANDRO-230617/214
Gain Information	16-05-2017	4.3	In TrustZone an information exposure vulnerability can potentially occur in all Android releases from CAF using the Linux kernel. **CVE ID: CVE-2015-9001**	https://source.android.com/security/bulletin/2017-04-01	O-GOO-ANDRO-230617/215
DoS Overflow	23-05-2017	5	Integer overflow in soundtrigger/ISoundTriggerHwService.cpp in Android allows attacks to cause a denial of service via unspecified vectors. **CVE ID: CVE-2015-1529**	https://android.googlesource.com/platform/frameworks/av/+/b9096dc	O-GOO-ANDRO-230617/216
DoS	12-05-2017	5.4	A denial of service vulnerability in libstagefright in Mediaserver could enable an attacker to use a specially crafted file to cause a device hang or reboot. This issue is rated as Moderate because it requires an uncommon device configuration. Product: Android. Versions: 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2. Android ID: A-35763994. **CVE ID: CVE-2017-0603**	https://android.googlesource.com/platform/frameworks/av/+/36b04932bb93cc3269279282686b439a17a89920	O-GOO-ANDRO-230617/217
Google;Linux					
Android/Linux Kernel					
Execute Code	12-05-2017	7.6	An elevation of privilege vulnerability in the Qualcomm Secure Channel Manager driver could enable a local malicious application to execute arbitrary code	https://source.android.com/security/bulletin/01-05-2017	O-GOO-ANDRO-230617/218

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

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

			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-35401052. References: QC-CR#1081711. **CVE ID: CVE-2017-0620**		
Execute Code	12-05-2017	7.6	An elevation of privilege vulnerability in the Qualcomm pin controller 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-35401152. References: QC-CR#826566. **CVE ID: CVE-2017-0619**	https://source.android.com/security/bulletin/01-05-2017	O-GOO-ANDRO-230617/219
Execute Code	12-05-2017	7.6	An elevation of privilege vulnerability in the Qualcomm ADSPRPC 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-34112914. References: QC-CR#1110747. **CVE ID: CVE-2017-0465**	https://source.android.com/security/bulletin/01-05-2017	O-GOO-ANDRO-230617/220
DoS Gain Privileges	02-05-2017	7.6	The regulator_ena_gpio_free function in drivers/regulator/core.c in the Linux kernel before 3.19 allows local users to gain privileges or cause a denial of service (use-after-free) via a crafted application. **CVE ID: CVE-2014-9940**	https://source.android.com/security/bulletin/01-05-2017	O-GOO-ANDRO-230617/221
Execute Code	02-05-2017	9.3	An elevation of privilege vulnerability in the NVIDIA video driver could enable a local malicious application to execute arbitrary code	https://source.android.com/security/bulletin/01-05-2017	O-GOO-ANDRO-230617/222

			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-34113000. References: N-CVE ID: CVE-2017-0331. **CVE ID: CVE-2017-0331**		
Gain Privileges	02-05-2017	9.3	kernel/events/core.c in the Linux kernel before 3.19 mishandles counter grouping, which allows local users to gain privileges via a crafted application, related to the perf_pmu_register and perf_event_open functions. **CVE ID: CVE-2015-9004**	https://source.android.com/security/bulletin/01-05-2017	O-GOO-ANDRO-230617/223
Microsoft					
Windows 10;Windows 7;Windows 8.1;Windows Rt 8.1;Windows Server 2008;Windows Server 2012;Windows Server 2016					
Gain Information	12-05-2017	4.3	Microsoft Server Message Block 1.0 (SMBv1) allows an information disclosure vulnerability in the way that Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 handles certain requests, aka "Windows SMB Information Disclosure Vulnerability". This CVE ID is unique from CVE-2017-0267, CVE-2017-0268, CVE-2017-0270, CVE-2017-0271, CVE-2017-0274, and CVE-2017-0275. **CVE ID: CVE-2017-0276**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0276	O-MIC-WINDO-230617/224
Mikrotik					
Routeros					
NA	18-05-2017	7.8	A vulnerability in MikroTik Version 6.38.5 could allow an	NA	O-MIK-ROUTE-

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

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

			unauthenticated remote attacker to exhaust all available CPU via a flood of UDP packets on port 500 (used for L2TP over IPsec), preventing the affected router from accepting new connections; all devices will be disconnected from the router and all logs removed automatically. **CVE ID: CVE-2017-8338**		230617/225
Mimosa					
Backhaul Radios;Client Radios					
Gain Information	21-05-2017	5	An information-leakage issue was discovered on Mimosa Client Radios before 2.2.3 and Mimosa Backhaul Radios before 2.2.3. There is a page in the web interface that will show you the device's serial number, regardless of whether or not you have logged in. This information-leakage issue is relevant because there is another page (accessible without any authentication) that allows you to remotely factory reset the device simply by entering the serial number. **CVE ID: CVE-2017-9134**	http://blog.iancaling.com/post/160596244178	O-MIM-BACKH-230617/226
Gain Information	21-05-2017	5	A hard-coded credentials issue was discovered on Mimosa Client Radios before 2.2.3, Mimosa Backhaul Radios before 2.2.3, and Mimosa Access Points before 2.2.3. These devices run Mosquitto, a lightweight message broker, to send information between devices. By using the vendor's hard-coded credentials to connect to the broker on any device (whether it be an AP, Client, or Backhaul model), an attacker can view all the messages being sent between the devices. If an attacker connects to an AP, the AP will leak information about any clients connected to it, including the serial	http://blog.iancaling.com/post/160596244178	O-MIM-BACKH-230617/227

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

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

			numbers, which can be used to remotely factory reset the clients via a page in their web interface. **CVE ID: CVE-2017-9132**		
Execute Code	21-05-2017	5	An issue was discovered on Mimosa Client Radios before 2.2.3 and Mimosa Backhaul Radios before 2.2.3. By connecting to the Mosquitto broker on an access point and one of its clients, an attacker can gather enough information to craft a command that reboots the client remotely when sent to the client's Mosquitto broker, aka "unauthenticated remote command execution." This command can be re-sent endlessly to act as a DoS attack on the client. **CVE ID: CVE-2017-9131**	http://blog.iancaling.com/post/160596244178	O-MIM-BACKH-230617/228
Gain Information	21-05-2017	7.8	An issue was discovered on Mimosa Client Radios before 2.2.3. In the device's web interface, there is a page that allows an attacker to use an unsanitized GET parameter to download files from the device as the root user. The attacker can download any file from the device's filesystem. This can be used to view unsalted, MD5-hashed administrator passwords, which can then be cracked, giving the attacker full admin access to the device's web interface. This vulnerability can also be used to view the plaintext pre-shared key (PSK) for encrypted wireless connections, or to view the device's serial number (which allows an attacker to factory reset the device). **CVE ID: CVE-2017-9136**	http://blog.iancaling.com/post/160596244178	O-MIM-BACKH-230617/229
Execute Code	21-05-2017	9	An issue was discovered on Mimosa Client Radios before 2.2.4 and Mimosa Backhaul Radios before 2.2.4. On the backend of the device's	http://blog.iancaling.com/post/160596244178	O-MIM-BACKH-230617/230

			web interface, there are some diagnostic tests available that are not displayed on the webpage; these are only accessible by crafting a POST request with a program like cURL. There is one test accessible via cURL that does not properly sanitize user input, allowing an attacker to execute shell commands as the root user. **CVE ID: CVE-2017-9135**		
Execute Code	21-05-2017	9	An issue was discovered on Mimosa Client Radios before 2.2.3 and Mimosa Backhaul Radios before 2.2.3. In the device's web interface, after logging in, there is a page that allows you to ping other hosts from the device and view the results. The user is allowed to specify which host to ping, but this variable is not sanitized server-side, which allows an attacker to pass a specially crafted string to execute shell commands as the root user. **CVE ID: CVE-2017-9133**	http://blog.iancaling.com/post/160596244178	O-MIM-BACKH-230617/231
Moxa					
Oncell 5004-hspa Firmware;Oncell 5104-hsdpa Firmware;Oncell 5104-hspa Firmware;Oncell G3110-hsdpa Firmware;Oncell G3110-hspa Firmware;Oncell G3150-hsdpa Firmware					
NA	29-05-2017	5	A Plaintext Storage of a Password issue was discovered in Moxa OnCell G3110-HSPA Version 1.3 build 15082117 and previous versions, OnCell G3110-HSDPA Version 1.2 Build 09123015 and previous versions, OnCell G3150-HSDPA Version 1.4 Build 11051315 and previous versions, OnCell 5104-HSDPA, OnCell 5104-HSPA, and OnCell 5004-HSPA. The application's configuration file contains parameters that represent passwords in plaintext. **CVE ID: CVE-2017-7913**	https://ics-cert.us-cert.gov/advisories/ICSA-17-143-01	O-MOX-ONCEL-230617/232
CSRF	29-05-2017	6.8	A Cross-Site Request Forgery issue was discovered in Moxa OnCell	https://ics-cert.us-	O-MOX-ONCEL-

			G3110-HSPA Version 1.3 build 15082117 and previous versions, OnCell G3110-HSDPA Version 1.2 Build 09123015 and previous versions, OnCell G3150-HSDPA Version 1.4 Build 11051315 and previous versions, OnCell 5104-HSDPA, OnCell 5104-HSPA, and OnCell 5004-HSPA. The application does not sufficiently verify if a request was intentionally provided by the user who submitted the request, which could allow an attacker to modify the configuration of the device. **CVE ID: CVE-2017-7917**	cert.gov/advisories/ICSA-17-143-01	230617/233
Bypass	29-05-2017	7.5	An Improper Restriction of Excessive Authentication Attempts issue was discovered in Moxa OnCell G3110-HSPA Version 1.3 build 15082117 and previous versions, OnCell G3110-HSDPA Version 1.2 Build 09123015 and previous versions, OnCell G3150-HSDPA Version 1.4 Build 11051315 and previous versions, OnCell 5104-HSDPA, OnCell 5104-HSPA, and OnCell 5004-HSPA. An attacker can freely use brute force to determine parameters needed to bypass authentication. **CVE ID: CVE-2017-7915**	https://ics-cert.us-cert.gov/advisories/ICSA-17-143-01	O-MOX-ONCEL-230617/234
Oneplus					
Oxygenos					
NA	11-05-2017	4.3	An issue was discovered on OnePlus One and X devices. Due to a lenient updater-script on the OnePlus One and X OTA images, the fact that both products use the same OTA verification keys, and the fact that both products share the same 'ro.build.product' system property, attackers can install OTAs of one product over the other, even on	https://alephsecurity.com/vulns/aleph-2017021	O-ONE-OXYGE-230617/235

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

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

			locked bootloaders. That could theoretically allow for exploitation of vulnerabilities patched on one image but not on the other, in addition to expansion of the attack surface. Moreover, the vulnerability may result in having the device unusable until a Factory Reset is performed. This vulnerability can be exploited by Man-in-the-Middle (MiTM) attackers targeting the update process. This is possible because the update transaction does not occur over TLS (CVE ID: CVE-2016-10370). In addition, physical attackers can reboot the phone into recovery, and then use 'adb sideload' to push the OTA. **CVE ID: CVE-2017-8851**		
NA	11-05-2017	4.3	An issue was discovered on OnePlus One, X, 2, 3, and 3T devices. Due to a lenient updater-script in the OnePlus OTA images, and the fact that both ROMs use the same OTA verification keys, attackers can install HydrogenOS over OxygenOS and vice versa, even on locked bootloaders, which allows for exploitation of vulnerabilities patched on one image but not on the other, in addition to expansion of the attack surface. This vulnerability can be exploited by Man-in-the-Middle (MiTM) attackers targeting the update process. This is possible because the update transaction does not occur over TLS (CVE ID: CVE-2016-10370). In addition, physical attackers can reboot the phone into recovery, and then use 'adb sideload' to push the OTA (on OnePlus 3/3T 'Secure Start-up' must be off). **CVE ID: CVE-2017-8850**	https://alephsecurity.com/vulns/aleph-2017020	O-ONE-OXYGE-230617/236
NA	11-05-2017	4.3	An issue was discovered on OnePlus	https://aleph	O-ONE-

			One, X, 2, 3, and 3T devices. OxygenOS and HydrogenOS are vulnerable to downgrade attacks. This is due to a lenient 'updater-script' in OTAs that does not check that the current version is lower than or equal to the given image's. Downgrades can occur even on locked bootloaders and without triggering a factory reset, allowing for exploitation of now-patched vulnerabilities with access to user data. This vulnerability can be exploited by a Man-in-the-Middle (MiTM) attacker targeting the update process. This is possible because the update transaction does not occur over TLS (CVE-2016-10370). In addition, a physical attacker can reboot the phone into recovery, and then use 'adb sideload' to push the OTA (on OnePlus 3/3T 'Secure Start-up' must be off). **CVE ID: CVE-2017-5948**	security.com/vulns/aleph-2017008	OXYGE-230617/237
NA	11-05-2017	5	An issue was discovered on OnePlus devices such as the 3T. The OnePlus OTA Updater pushes the signed-OTA image over HTTP without TLS. While it does not allow for installation of arbitrary OTAs (due to the digital signature), it unnecessarily increases the attack surface, and allows for remote exploitation of other vulnerabilities such as CVE-2017-5948, CVE-2017-8850, and CVE-2017-8851. **CVE ID: CVE-2016-10370**		O-ONE-OXYGE-230617/238
OS/ Application					
Apple/Apple					
Iphone Os/Safari					
XSS	22-05-2017	4.3	An issue was discovered in certain Apple products. iOS before 10.3.2 is affected. Safari before 10.1.1 is	https://support.apple.com/HT207804	O-A-APP-IPHON-

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

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

			affected. The issue involves the "WebKit" component. It allows remote attackers to conduct Universal XSS (UXSS) attacks via a crafted web site that improperly interacts with cached frames. **CVE ID: CVE-2017-2528**		230617/239
XSS	22-05-2017	4.3	An issue was discovered in certain Apple products. iOS before 10.3.2 is affected. Safari before 10.1.1 is affected. The issue involves the "WebKit" component. It allows remote attackers to conduct Universal XSS (UXSS) attacks via a crafted web site that improperly interacts with pageshow events. **CVE ID: CVE-2017-2510**	https://support.apple.com/HT207804	O-A-APP-IPHON-230617/240
Debian;Fedoraproject;Novell;Opensuse Project;Redhat/Google					
Debian Linux/Fedora/Leap/Opensuse/Enterprise Linux Server Supplementary;Enterprise Linux Workstation Supplementary/Chrome					
DoS	23-05-2017	7.5	Multiple unspecified vulnerabilities in Google Chrome before 53.0.2785.143 allow remote attackers to cause a denial of service or possibly have other impact via unknown vectors. **CVE ID: CVE-2016-5178**	https://chromereleases.googleblog.com/2016/09/stable-channel-update-for-desktop_29.html	O-A-DEB-DEBIA-230617/241

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

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable