Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Application (A)					
Afterlogic					
Aurora;Webmail					
XSS	19-09-2017	3.5	AdminPanel in AfterLogic WebMail 7.7 and Aurora 7.7.5 has XSS via the txtDomainName field to adminpanel/modules/pro/inc/ajax.php during addition of a domain. **CVE ID:CVE-2017-14597**	https://auroramail.wordpress.com/2017/08/28/vulnerability-in-webmailaurora-closed/	A-AFT-AUROR-011017/1
Antisamy Project					
Antisamy					
XSS	25-09-2017	4.3	OWASP AntiSamy through 1.5.7 allows XSS via HTML5 entities, as demonstrated by use of : to construct a javascript: URL. **CVE ID:CVE-2017-14735**	https://github.com/nahsra/antisamy/issues/10	A-ANT-ANTIS-011017/2
Apache					
Struts					
NA	20-09-2017	4.3	In Apache Struts 2.5 through 2.5.5, if an application allows entering a URL in a form field and the built-in URLValidator is used, it is possible to prepare a special URL which will be used to overload server process when performing validation of the URL**CVE ID:.CVE-2016-8738**	https://struts.apache.org/docs/s2-044.html	A-APA-STRUT-011017/3
XSS	25-09-2017	4.3	Cross-site scripting (XSS) vulnerability in Apache Struts before 2.3.20. **CVE ID:CVE-2015-5169**	https://struts.apache.org/docs/s2-025.html	A-APA-STRUT-011017/4
Tomcat					
Bypass Gain Information	19-09-2017	5	When using a VirtualDirContext with Apache Tomcat 7.0.0 to 7.0.80	NA	A-APA-TOMCA-

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

			it was possible to bypass security constraints and/or view the source code of JSPs for resources served by the VirtualDirContext using a specially crafted request. **CVE ID:CVE-2017-12616**		011017/5
Solr					
NA	18-09-2017	6	Solr's Kerberos plugin can be configured to use delegation tokens, which allows an application to reuse the authentication of an end-user or another application. There are two issues with this functionality (when using SecurityAwareZkACLProvider type of ACL provider e.g. SaslZkACLProvider). Firstly, access to the security configuration can be leaked to users other than the solr super user. Secondly, malicious users can exploit this leaked configuration for privilege escalation to further expose/modify private data and/or disrupt operations in the Solr cluster. The vulnerability is fixed from Solr 6.6.1 onwards. **CVE ID:CVE-2017-9803**	NA	A-APA-SOLR-011017/6
Tomcat					
Execute Code	19-09-2017	6.8	When running Apache Tomcat 7.0.0 to 7.0.79 on Windows with HTTP PUTs enabled (e.g. via setting the readonly initialisation parameter of the Default to false) it was possible to upload a JSP file to the server via a specially crafted request. This JSP could then be requested and any code it contained would be executed by the server. **CVE ID:CVE-2017-12615**	NA	A-APA-TOMCA-011017/7
Struts					

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	20-09-2017	7.5	In Apache Struts 2.0.1 through 2.3.33 and 2.5 through 2.5.10, using an unintentional expression in a Freemarker tag instead of string literals can lead to a RCE attack. **CVE ID:CVE-2017-12611**	https://struts.apache.org/docs/s2-053.html	A-APA-STRUT-011017/8
Execute Code Dir. Trav.	20-09-2017	7.5	In the Convention plugin in Apache Struts 2.3.20 through 2.3.30, it is possible to prepare a special URL which will be used for path traversal and execution of arbitrary code on server side. **CVE ID:CVE-2016-6795**	https://struts.apache.org/docs/s2-042.html	A-APA-STRUT-011017/9
Artifex					
Mupdf					
DoS Overflow	22-09-2017	6.8	Artifex MuPDF 1.11 allows attackers to cause a denial of service or possibly have unspecified other impact via a crafted .xps file, related to "Data from Faulting Address controls Branch Selection starting at mupdf+0x000000000016cb4f" on Windows. This occurs because of mishandling of XML tag name comparisons. **CVE ID:CVE-2017-14687**	NA	A-ART-MUPDF-011017/10
DoS Execute Code Overflow	22-09-2017	6.8	Artifex MuPDF 1.11 allows attackers to execute arbitrary code or cause a denial of service via a crafted .xps file, related to a "User Mode Write AV near NULL starting at wow64!Wow64NotifyDebugger+0x000000000000001d" on Windows. This occurs because read_zip_dir_imp in fitz/unzip.c does not check whether size fields in a ZIP entry are negative numbers. **CVE ID:CVE-2017-14686**	NA	A-ART-MUPDF-011017/11
DoS Overflow	22-09-2017	6.8	Artifex MuPDF 1.11 allows attackers to cause a denial of	NA	A-ART-MUPDF-

			service or possibly have unspecified other impact via a crafted .xps file, related to "Data from Faulting Address controls Branch Selection starting at mupdf+0x000000000016aa61" on Windows. This occurs because xps_load_links_in_glyphs in xps/xps-link.c does not verify that an xps font could be loaded. **CVE ID:CVE-2017-14685**		011017/12
Bareos					
Bareos					
Execute Code	20-09-2017	4.6	bareos-dir, bareos-fd, and bareos-sd in bareos-core in Bareos 16.2.6 and earlier create a PID file after dropping privileges to a non-root account, which might allow local users to kill arbitrary processes by leveraging access to this non-root account for PID file modification before a root script executes a "kill `cat /pathname`" command. **CVE ID: CVE-2017-14610**	https://bugs.bareos.org/view.php?id=847	A-BAR-BAREO-011017/13
Bento4					
Bento4					
DoS Overflow	21-09-2017	4.3	A heap-based buffer over-read was discovered in AP4_BitStream::ReadBytes in Codecs/Ap4BitStream.cpp in Bento4 version 1.5.0-617. The vulnerability causes an application crash, which leads to remote denial of service. **CVE ID: CVE-2017-14645**	https://blogs.gentoo.org/ago/2017/09/14/bento4-heap-based-buffer-overflow-in-ap4_bitstreamreadbytes-ap4bitstream-cpp/	A-BEN-BENTO-011017/14
Overflow	21-09-2017	4.3	The AP4_HdlrAtom class in	NA	A-BEN-

			Core/Ap4HdlrAtom.cpp in Bento4 version 1.5.0-617 uses an incorrect character data type, leading to a heap-based buffer over-read and application crash in AP4_BytesToUInt32BE in Core/Ap4Utils.h. **CVE ID: CVE-2017-14643**		BENTO-011017/15
DoS	21-09-2017	4.3	A NULL pointer dereference was discovered in the AP4_HdlrAtom class in Bento4 version 1.5.0-617. The vulnerability causes a segmentation fault and application crash in AP4_StdcFileByteStream::ReadPartial in System/StdC/Ap4StdCFileByteStream.cpp, which leads to remote denial of service. **CVE ID: CVE-2017-14642**	NA	A-BEN-BENTO-011017/16
DoS	21-09-2017	4.3	A NULL pointer dereference was discovered in the AP4_DataAtom class in MetaData/Ap4MetaData.cpp in Bento4 version 1.5.0-617. The vulnerability causes a segmentation fault and application crash, which leads to remote denial of service. **CVE ID: CVE-2017-14641**	NA	A-BEN-BENTO-011017/17
DoS	21-09-2017	4.3	A NULL pointer dereference was discovered in AP4_AtomSampleTable::GetSample in Core/Ap4AtomSampleTable.cpp in Bento4 version 1.5.0-617. The vulnerability causes a segmentation fault and application crash, which leads to remote denial of service. **CVE ID: CVE-2017-14640**	NA	A-BEN-BENTO-011017/18
NA	21-09-2017	4.3	AP4_AtomFactory::CreateAtomFromStream in Core/Ap4AtomFactory.cpp in	NA	A-BEN-BENTO-011017/19

			Bento4 version 1.5.0-617 has missing NULL checks, leading to a NULL pointer dereference, segmentation fault, and application crash in AP4_Atom::SetType in Core/Ap4Atom.h. **CVE ID: CVE-2017-14638**		
Overflow	21-09-2017	5	The AP4_AvccAtom and AP4_HvccAtom classes in Bento4 version 1.5.0-617 do not properly validate data sizes, leading to a heap-based buffer over-read and application crash in AP4_DataBuffer::SetData in Core/Ap4DataBuffer.cpp. **CVE ID: CVE-2017-14646**	NA	A-BEN-BENTO-011017/20
DoS Execute Code Overflow	21-09-2017	6.8	A heap-based buffer overflow was discovered in AP4_VisualSampleEntry::ReadFields in Core/Ap4SampleEntry.cpp in Bento4 1.5.0-617. The vulnerability causes an out-of-bounds write, which leads to remote denial of service or possibly code execution. **CVE ID: CVE-2017-14647**	https://blogs.gentoo.org/ago/2017/09/14/bento4-stack-based-buffer-overflow-in-ap4_visualsampleentryreadfields-ap4sampleentry-cpp/	A-BEN-BENTO-011017/21
DoS Execute Code Overflow	21-09-2017	6.8	A heap-based buffer overflow was discovered in the AP4_HdlrAtom class in Bento4 1.5.0-617. The vulnerability causes an out-of-bounds write, which leads to remote denial of service or possibly code execution. **CVE ID: CVE-2017-14644**	https://blogs.gentoo.org/ago/2017/09/14/bento4-heap-based-buffer-overflow-in-ap4_hdlratomap4_hdl	A-BEN-BENTO-011017/22

				ratom-ap4hdlratom-cpp/	
DoS Overflow	21-09-2017	6.8	AP4_VisualSampleEntry::ReadFields in Core/Ap4SampleEntry.cpp in Bento4 1.5.0-617 uses incorrect character data types, which causes a stack-based buffer underflow and out-of-bounds write, leading to denial of service (application crash) or possibly unspecified other impact. **CVE ID: CVE-2017-14639**	NA	A-BEN-BENTO-011017/23
Bladeenc					
Bladeenc					
DoS Execute Code Overflow	21-09-2017	7.5	A global buffer overflow was discovered in the iteration_loop function in loop.c in BladeEnc version 0.94.2. The vulnerability causes an out-of-bounds write, which leads to remote denial of service or possibly code execution. **CVE ID: CVE-2017-14648**	https://blogs.gentoo.org/ago/2017/09/19/bladeenc-global-buffer-overflow-in-iteration_loop-loop-c/	A-BLA-BLADE-011017/24
Cisco					
Findit Network Discovery Utility					
NA	21-09-2017	4.6	A vulnerability in the Cisco FindIT Network Discovery Utility could allow an authenticated, local attacker to perform a DLL preloading attack, potentially causing a partial impact to device availability, confidentiality, and integrity. The vulnerability is due to the application loading a malicious copy of a specific, nondefined DLL file instead of the DLL file it was expecting. An attacker could exploit this vulnerability by placing an affected DLL within the search path of the host system. An exploit could allow the attacker to load a malicious	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170920-findit	A-CIS-FINDI-011017/25

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

			DLL file into the system, thus partially compromising confidentiality, integrity, and availability on the device. Cisco Bug IDs: CSCve89785. **CVE ID: CVE-2017-12252**		
Cloud Web Security					
Overflow Bypass	19-09-2017	5	Cisco Cloud Web Security before 3.0.1.7 allows remote attackers to bypass intended filtering protection mechanisms by leveraging improper handling of HTTP methods, aka Bug ID CSCut69743. **CVE ID: CVE-2015-0689**	https://tools.cisco.com/security/center/viewAlert.x?alertId=38221	A-CIS-CLOUD-011017/26
Wide Area Application Services					
DoS	21-09-2017	5	A vulnerability in the HTTP web interface for Cisco Wide Area Application Services (WAAS) could allow an unauthenticated, remote attacker to cause an HTTP Application Optimization (AO) related process to restart, causing a partial denial of service (DoS) condition. The vulnerability is due to lack of input validation of user-supplied input parameters within an HTTP request. An attacker could exploit this vulnerability by sending a crafted HTTP request through the targeted device. An exploit could allow the attacker to cause a DoS condition due to a process unexpectedly restarting. The WAAS could drop traffic during the brief time the process is restarting. Cisco Bug IDs: CSCvc63048. **CVE ID: CVE-2017-12250**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170920-waas	A-CIS-WIDE - 011017/27
Unified Customer Voice Portal					
Gain Privileges	21-09-2017	6.5	A vulnerability in the Operations, Administration, Maintenance, and	https://tools.cisco.com/secu	A-CIS-UNIFI-

			Provisioning (OAMP) credential reset functionality for Cisco Unified Customer Voice Portal (CVP) could allow an authenticated, remote attacker to gain elevated privileges. The vulnerability is due to a lack of proper input validation. An attacker could exploit this vulnerability by authenticating to the OAMP and sending a crafted HTTP request. A successful exploit could allow the attacker to gain administrator privileges. The attacker must successfully authenticate to the system to exploit this vulnerability. This vulnerability affects Cisco Unified Customer Voice Portal (CVP) running software release 10.5, 11.0, or 11.5. Cisco Bug IDs: CSCve92752. **CVE ID: CVE-2017-12214**	rity/center/content/CiscoSecurityAdvisory/cisco-sa-20170920-cvp	011017/28
Unified Computing System					
NA	21-09-2017	7.2	A vulnerability in the CLI of Cisco UCS Central Software could allow an authenticated, local attacker to gain shell access. The vulnerability is due to insufficient input validation of commands entered in the CLI, aka a Restricted Shell Break Vulnerability. An attacker could exploit this vulnerability by entering a specific command with crafted arguments. An exploit could allow the attacker to gain shell access to the underlying system. Cisco Bug IDs: CSCve70762. **CVE ID: CVE-2017-12255**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170920-ucs	A-CIS-UNIFI-011017/29
Codeigniter					
Codeigniter					
NA	19-09-2017	5	CodeIgniter before 2.2.0 makes it easier for attackers to decode	https://codeigniter.com/user	A-COD-CODEI-

			session cookies by leveraging fallback to a custom XOR-based encryption scheme when the Mcrypt extension for PHP is not available. **CVE ID: CVE-2014-8686**	guide2/changelog.html	011017/30
Codeigniter;Kohanaframework					
Codeigniter/Kohana					
NA	19-09-2017	7.5	CodeIgniter before 3.0 and Kohana 3.2.3 and earlier and 3.3.x through 3.3.2 make it easier for remote attackers to spoof session cookies and consequently conduct PHP object injection attacks by leveraging use of standard string comparison operators to compare cryptographic hashes. **CVE ID: CVE-2014-8684**	https://github.com/kohana/core/pull/492	A-COD-CODEI-011017/31
Comicsmart					
Ganma!					
NA	25-09-2017	4	GANMA! App for iOS does not verify SSL certificates. **CVE ID: CVE-2015-7785**	NA	A-COM-GANMA-011017/32
Crony Cronjob Manager Project					
Crony Cronjob Manager					
XSS CSRF	17-09-2017	6	WP_Admin_UI in the Crony Cronjob Manager plugin before 0.4.7 for WordPress has CSRF via the name parameter in an action=manage&do=create operation, as demonstrated by inserting XSS sequences. **CVE ID: CVE-2017-14530**	NA	A-CRO-CRONY-011017/33
Cyberlink					
Labelprint					
Execute Code Overflow	23-09-2017	6.8	Stack-based buffer overflows in CyberLink LabelPrint 2.5 allow remote attackers to execute arbitrary code via the (1) author (inside the INFORMATION tag), (2) name (inside the INFORMATION tag), (3) artist (inside the TRACK	NA	A-CYB-LABEL-011017/34

			tag), or (4) default (inside the TEXT tag) parameter in an lpp project file. **CVE ID: CVE-2017-14627**		
Dovecot					
Dovecot					
DoS	19-09-2017	4.3	The ssl-proxy-openssl.c function in Dovecot before 2.2.17, when SSLv3 is disabled, allow remote attackers to cause a denial of service (login process crash) via vectors related to handshake failures. **CVE ID: CVE-2015-3420**	https://bugzilla.redhat.com/show_bug.cgi?id=1216057	A-DOV-DOVEC-011017/35
Emberjs					
Ember.js					
XSS	20-09-2017	4.3	Cross-site scripting (XSS) vulnerability in Ember.js 1.10.x before 1.10.1 and 1.11.x before 1.11.2. **CVE ID: CVE-2015-1866**	https://emberjs.com/blog/2015/04/14/security-and-bugfix-releases-ember-1-10-1-1-11-2-1-11-3.html	A-EMB-EMBER-011017/36
Exiv2					
Exiv2					
DoS Overflow	28-09-2017	4.3	There is a heap-based buffer overflow in the Exiv2::s2Data function of types.cpp in Exiv2 0.26. A Crafted input will lead to a denial of service attack. **CVE ID: CVE-2017-14866**	https://bugzilla.redhat.com/show_bug.cgi?id=1494781	A-EXI-EXIV2-011017/37
DoS Overflow	28-09-2017	4.3	There is a heap-based buffer overflow in the Exiv2::us2Data function of types.cpp in Exiv2 0.26. A Crafted input will lead to a denial of service attack. **CVE ID: CVE-2017-14865**	https://bugzilla.redhat.com/show_bug.cgi?id=1494778	A-EXI-EXIV2-011017/38
DoS Overflow	28-09-2017	4.3	An Invalid memory address dereference was discovered in Exiv2::getULong in types.cpp in Exiv2 0.26. The vulnerability causes a segmentation fault and	https://bugzilla.redhat.com/show_bug.cgi?id=1494467	A-EXI-EXIV2-011017/39

			application crash, which leads to denial of service. **CVE ID: CVE-2017-14864**		
DoS Overflow	28-09-2017	4.3	A NULL pointer dereference was discovered in Exiv2::Image::printIFDStructure in image.cpp in Exiv2 0.26. The vulnerability causes a segmentation fault and application crash, which leads to denial of service. **CVE ID: CVE-2017-14863**	https://bugzilla.redhat.com/show_bug.cgi?id=1494443	A-EXI-EXIV2-011017/40
DoS Overflow	28-09-2017	4.3	An Invalid memory address dereference was discovered in Exiv2::DataValue::read in value.cpp in Exiv2 0.26. The vulnerability causes a segmentation fault and application crash, which leads to denial of service. **CVE ID: CVE-2017-14862**	https://bugzilla.redhat.com/show_bug.cgi?id=1494786	A-EXI-EXIV2-011017/41
DoS	28-09-2017	4.3	There is a stack consumption vulnerability in the Exiv2::Internal::stringFormat function of image.cpp in Exiv2 0.26. A Crafted input will lead to a remote denial of service attack. **CVE ID:CVE-2017-14861**	https://bugzilla.redhat.com/show_bug.cgi?id=1494787	A-EXI-EXIV2-011017/42
DoS Overflow	28-09-2017	4.3	There is a heap-based buffer over-read in the Exiv2::Jp2Image::readMetadata function of jp2image.cpp in Exiv2 0.26. A Crafted input will lead to a denial of service attack. **CVE-2017-14860**	https://bugzilla.redhat.com/show_bug.cgi?id=1494776	A-EXI-EXIV2-011017/43
DoS Overflow	28-09-2017	4.3	An Invalid memory address dereference was discovered in Exiv2::StringValueBase::read in value.cpp in Exiv2 0.26. The vulnerability causes a segmentation fault and application crash, which leads to denial of service. **CVE ID: CVE-2017-14859**	https://bugzilla.redhat.com/show_bug.cgi?id=1494780	A-EXI-EXIV2-011017/44

DoS Overflow	28-09-2017	4.3	There is a heap-based buffer overflow in the Exiv2::l2Data function of types.cpp in Exiv2 0.26. A Crafted input will lead to a denial of service attack. **CVE ID: CVE-2017-14858**	https://bugzilla.redhat.com/show_bug.cgi?id=1494782	A-EXI-EXIV2-011017/45
DoS	28-09-2017	4.3	In Exiv2 0.26, there is an invalid free in the Image class in image.cpp that leads to a Segmentation fault. A crafted input will lead to a denial of service attack. **CVE ID: CVE-2017-14857**	https://bugzilla.redhat.com/show_bug.cgi?id=1495043	A-EXI-EXIV2-011017/46
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 Link Controller;Big-ip Local Traffic Manager;Big-ip Policy Enforcement Manager;Big-ip Websafe					
NA	18-09-2017	4.3	In F5 BIG-IP LTM, AAM, AFM, Analytics, APM, ASM, DNS, Link Controller, PEM, and WebSafe 12.1.2-HF1 and 13.0.0, an undisclosed type of responses may cause TMM to restart, causing an interruption of service when "SSL Forward Proxy" setting is enabled in both the Client and Server SSL profiles assigned to a BIG-IP Virtual Server. **CVE ID: CVE-2017-6147**	https://support.f5.com/csp/article/K43945001	A-F5-BIG-I-011017/47
Ffmpeg					
Ffmpeg					
DoS Overflow	27-09-2017	6.8	The sdp_parse_fmtp_config_h264 function in libavformat/rtpdec_h264.c in FFmpeg before 3.3.4 mishandles empty sprop-parameter-sets values, which allows remote attackers to cause a denial of service (heap buffer overflow) or possibly have unspecified other impact via a crafted sdp file. **CVE ID: CVE-2017-14767**	https://github.com/FFmpeg/FFmpeg/commit/c42a1388a6d1bfd8001bf6a4241d8ca27e49326d	A-FFM-FFMPE-011017/48
Floating Social Bar 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

Floating Social Bar					
XSS	19-09-2017	4.3	Cross-site scripting (XSS) vulnerability in the Floating Social Bar plugin before 1.1.7 for WordPress allows remote attackers to inject arbitrary web script or HTML via vectors related to original service order. **CVE ID: CVE-2015-3299**	https://plugins.trac.wordpress.org/changeset/1129648/floating-social-bar/trunk	A-FLO-FLOAT-011017/49
Foxitsoftware					
Foxit Reader					
DoS Execute Code Overflow	22-09-2017	4.6	Foxit Reader 8.3.2.25013 allows attackers to execute arbitrary code or cause a denial of service via a crafted .pdf file, related to "Data from Faulting Address controls Code Flow starting at tiptsf!CPenInputPanel::FinalRelease+0x000000000000002f." **CVE ID: CVE-2017-14694**	NA	A-FOX-FOXIT-011017/50
Freedesktop					
Poppler					
NA	17-09-2017	4.3	In Poppler 0.59.0, a NULL Pointer Dereference exists in the XRef::parseEntry() function in XRef.cc via a crafted PDF document. **CVE ID: CVE-2017-14517**	https://bugs.freedesktop.org/show_bug.cgi?id=102687	A-FRE-POPPL-011017/51
NA	29-09-2017	4.3	In Poppler 0.59.0, a NULL Pointer Dereference exists in AnnotRichMedia::Configuration::Configuration in Annot.cc via a crafted PDF document. **CVE ID: CVE-2017-14928**	https://bugs.freedesktop.org/show_bug.cgi?id=102607	A-FRE-POPPL-011017/52
NA	29-09-2017	4.3	In Poppler 0.59.0, a NULL Pointer Dereference exists in the SplashOutputDev ::type3 D0() function in SplashOutput Dev.cc via a crafted PDF document. **CVE ID: CVE-2017-14927**	https://bugs.freedesktop.org/show_bug.cgi?id=102604	A-FRE-POPPL-011017/53
NA	29-09-2017	4.3	In Poppler 0.59.0, a NULL Pointer Dereference exists in AnnotRichMedia::Content::Content	https://bugs.freedesktop.org/show_bug.cgi	A-FRE-POPPL-011017

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

			in Annot.cc via a crafted PDF document. **CVE ID: CVE-2017-14926**	?id=102601	/54
Overflow Mem. Corr.	17-09-2017	5	In Poppler 0.59.0, memory corruption occurs in a call to Object::streamGetChar in Object.h after a repeating series of Gfx::display, Gfx::go, Gfx::execOp, Gfx::opShowText, and Gfx::doShowText calls (aka a Gfx.cc infinite loop). **CVE ID: CVE-2017-14519**	https://bugs.freedesktop.org/show_bug.cgi?id=102701	A-FRE-POPPL-011017/55
NA	17-09-2017	6.8	In Poppler 0.59.0, a floating point exception occurs in Splash::scaleImageYuXd() in Splash.cc, which may lead to a potential attack when handling malicious PDF files. **CVE ID:CVE-2017-14520**	https://bugs.freedesktop.org/show_bug.cgi?id=102719	A-FRE-POPPL-011017/56
NA	17-09-2017	6.8	In Poppler 0.59.0, a floating point exception exists in the isImageInterpolationRequired() function in Splash.cc via a crafted PDF document. **CVE ID: CVE-2017-14518**	https://bugs.freedesktop.org/show_bug.cgi?id=102688	A-FRE-POPPL-011017/57
NA	20-09-2017	6.8	In Poppler 0.59.0, a floating point exception occurs in the ImageStream class in Stream.cc, which may lead to a potential attack when handling malicious PDF files. **CVE ID: CVE-2017-14617**	https://bugs.freedesktop.org/show_bug.cgi?id=102854	A-FRE-POPPL-011017/58
Freeipa					
Freeipa					
NA	20-09-2017	5	FreeIPA might display user data improperly via vectors involving non-printable characters. **CVE ID: CVE-2015-5179**	https://bugzilla.redhat.com/show_bug.cgi?id=1252567	A-FRE-FREEI-011017/59
Gain Information	21-09-2017	5	ipa-kra-install in FreeIPA before 4.2.2 puts the CA agent certificate and private key in /etc/httpd/alias/kra-agent.pem,	https://pagure.io/freeipa/issue/5347	A-FRE-FREEI-011017/60

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

			which is world readable. **CVE ID: CVE-2015-5284**		
Geminabox Project					
Geminabox					
XSS	25-09-2017	3.5	geminabox (aka Gem in a Box) before 0.13.6 has XSS, as demonstrated by uploading a gem file that has a crafted gem.homepage value in its .gemspec file. **CVE ID: CVE-2017-14506**	NA	A-GEM-GEMIN-011017/61
CSRF	25-09-2017	6.8	geminabox (aka Gem in a Box) before 0.13.7 has CSRF, as demonstrated by an unintended gem upload. **CVE ID: CVE-2017-14683**	NA	A-GEM-GEMIN-011017/62
Genixcms					
Genixcms					
XSS	27-09-2017	4.3	In GeniXCMS 1.1.4, gxadmin/index.php has XSS via the Menu ID field in a page=menus request. **CVE ID: CVE-2017-14765**	http://ph0rse.me/2017/09/21/GeniXCMS-1-1-4%E6%9C%80%E6%96%B0%E7%89%88%E6%9C%AC-getshell/	A-GEN-GENIX-011017/63
XSS	27-09-2017	4.3	In GeniXCMS 1.1.4, /inc/lib/Control/Backend/menus.control.php has XSS via the id parameter. **CVE ID: CVE-2017-14762**	http://ph0rse.me/2017/09/21/GeniXCMS-1-1-4%E6%9C%80%E6%96%B0%E7%89%88%E6%9C%AC-getshell/	A-GEN-GENIX-011017/64
XSS	27-09-2017	4.3	In GeniXCMS 1.1.4, /inc/lib/backend/menus.control.php has XSS via the id parameter. **CVE ID: CVE-2017-14761**	http://ph0rse.me/2017/09/21/GeniXCMS-1-1-4%E6%9C%80%E6%96%B	A-GEN-GENIX-011017/65

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

				0%E7%89%88%E6%9C%AC-getshell/	
Execute Code	27-09-2017	6.5	In the Upload Modules page in GeniXCMS 1.1.4, remote authenticated users can execute arbitrary PHP code via a .php file in a ZIP archive of a module. **CVE ID: CVE-2017-14764**	http://ph0rse.me/2017/09/21/GeniXCMS-1-1-4%E6%9C%80%E6%96%B0%E7%89%88%E6%9C%AC-getshell/	A-GEN-GENIX-011017/66
Execute Code	27-09-2017	6.5	In the Install Themes page in GeniXCMS 1.1.4, remote authenticated users can execute arbitrary PHP code via a .php file in a ZIP archive of a theme. **CVE ID: CVE-2017-14763**	http://ph0rse.me/2017/09/21/GeniXCMS-1-1-4%E6%9C%80%E6%96%B0%E7%89%88%E6%9C%AC-getshell/	A-GEN-GENIX-011017/67
GNU					
Coreutils					
NA	20-09-2017	3.3	fts.c in coreutils 8.4 allows local users to delete arbitrary files. **CVE ID: CVE-2015-1865**	https://bugzilla.redhat.com/show_bug.cgi?id=1211300	A-GNU-COREU-011017/68
Binutils					
DoS Overflow	17-09-2017	4.3	The pe_print_idata function in peXXigen.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, mishandles HintName vector entries, which allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted PE file, related to the bfd_getl16 function. **CVE ID: CVE-2017-14529**	https://sourceware.org/bugzilla/show_bug.cgi?id=22113	A-GNU-BINUT-011017/69
DoS	29-09-2017	4.3	scan_unit_for_symbols in dwarf2.c in the Binary File Descriptor (BFD)	NA	A-GNU-BINUT-

			library (aka libbfd), as distributed in GNU Binutils 2.29, allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted ELF file. **CVE ID: CVE-2017-14940**		011017/70
DoS Overflow	29-09-2017	4.3	decode_line_info in dwarf2.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, mishandles a length calculation, which allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted ELF file, related to read_1_byte. **CVE ID: CVE-2017-14939**	NA	A-GNU-BINUT-011017/71
DoS	29-09-2017	4.3	_bfd_elf_slurp_version_tables in elf.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, allows remote attackers to cause a denial of service (excessive memory allocation and application crash) via a crafted ELF file. **CVE ID: CVE-2017-14938**	NA	A-GNU-BINUT-011017/72
DoS	29-09-2017	4.3	read_formatted_entries in dwarf2.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, allows remote attackers to cause a denial of service (infinite loop) via a crafted ELF file. **CVE ID: CVE-2017-14933**	https://sourceware.org/git/gitweb.cgi?p=binutils-gdb.git;h=33e0a9a056bd23e923b929a4f2ab049ade0b1c32	A-GNU-BINUT-011017/73
DoS	29-09-2017	4.3	decode_line_info in dwarf2.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, allows remote attackers to cause a denial of service (infinite loop) via a crafted ELF file. **CVE ID: CVE-2017-14932**	https://sourceware.org/git/gitweb.cgi?p=binutils-gdb.git;h=e3388894dc2e603683bed2172e8e9f25b29051005	A-GNU-BINUT-011017/74

DoS Overflow	25-09-2017	6.8	The *_get_synthetic_symtab functions in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, do not ensure a unique PLT entry for a symbol, which allows remote attackers to cause a denial of service (heap-based buffer overflow and application crash) or possibly have unspecified other impact via a crafted ELF file, related to elf32-i386.c and elf64-x86-64.c. **CVE ID: CVE-2017-14729**	NA	A-GNU-BINUT-011017/75
DoS Overflow	2017-09-26	6.8	The *_get_synthetic_symtab functions in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, interpret a -1 value as a sorting count instead of an error flag, which allows remote attackers to cause a denial of service (integer overflow and application crash) or possibly have unspecified other impact via a crafted ELF file, related to elf32-i386.c and elf64-x86-64.c. **CVE ID: CVE-2017-14745**	https://sourceware.org/bugzilla/show_bug.cgi?id=22148	A-GNU-BINUT-011017/76
DoS	29-09-2017	7.1	Memory leak in decode_line_info in dwarf2.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, allows remote attackers to cause a denial of service (memory consumption) via a crafted ELF file. **CVE ID: CVE-2017-14930**	https://sourceware.org/bugzilla/show_bug.cgi?id=22191	A-GNU-BINUT-011017/77
Good					
Good For Enterprise					
NA	20-09-2017	2.6	The Good for Enterprise application 3.0.0.415 for Android does not use signature protection for its Authentication Delegation	NA	A-GOO-GOOD - 011017/78

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

			API intent. Also, the Good Dynamic application activation process does not attempt to detect malicious activation attempts involving modified names beginning with a com.good.gdgma substring. Consequently, an attacker could obtain access to intranet data. This issue is only relevant in cases where the user has already downloaded a malicious Android application. **CVE ID: CVE-2015-9232**		
Graphicsmagick					
Graphicsmagick					
NA	17-09-2017	4.3	ReadPNMImage in coders/pnm.c in GraphicsMagick 1.3.26 does not ensure the correct number of colors for the XV 332 format, leading to a NULL Pointer Dereference. **CVE ID: CVE-2017-14504**	https://sourceforge.net/p/graphicsmagick/bugs/466/	A-GRA-GRAPH-011017/79
DoS	21-09-2017	4.3	ReadOneJNGImage in coders/png.c in GraphicsMagick version 1.3.26 does not properly validate JNG data, leading to a denial of service (assertion failure in magick/pixel_cache.c, and application crash). **CVE ID: CVE-2017-14649**	NA	A-GRA-GRAPH-011017/80
DoS Overflow	25-09-2017	4.3	ReadRLEImage in coders/rle.c in GraphicsMagick 1.3.26 mishandles RLE headers that specify too few colors, which allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted file. **CVE ID:CVE-2017-14733**	https://sourceforge.net/p/graphicsmagick/bugs/458/	A-GRA-GRAPH-011017/81
Helpdesk Pro Project					
Helpdesk Pro					
XSS	20-09-2017	3.5	Multiple cross-site scripting (XSS)	NA	A-HEL-

			vulnerabilities in the Helpdesk Pro plugin before 1.4.0 for Joomla! allow remote attackers to inject arbitrary web script or HTML via vectors related to name and message. **CVE ID: CVE-2015-4072**		HELPD-011017/82
Dir. Trav.	20-09-2017	5	Directory traversal vulnerability in the Helpdesk Pro plugin before 1.4.0 for Joomla! allows remote attackers to read arbitrary files via a .. (dot dot) in the filename parameter in a ticket.download_attachment task. **CVE ID: CVE-2015-4074**	NA	A-HEL-HELPD-011017/83
NA	20-09-2017	6.8	The Helpdesk Pro plugin before 1.4.0 for Joomla! allows remote attackers to write to arbitrary .ini files via a crafted language.save task. **CVE ID: CVE-2015-4075**	NA	A-HEL-HELPD-011017/84
Execute Code Sql	20-09-2017	7.5	Multiple SQL injection vulnerabilities in the Helpdesk Pro plugin before 1.4.0 for Joomla! allow remote attackers to execute arbitrary SQL commands via the (1) ticket_code or (2) email parameter or (3) remote authenticated users to execute arbitrary SQL commands via the filter_order parameter. **CVE ID: CVE-2015-4073**	NA	A-HEL-HELPD-011017/85
IBM					
Business Process Manager					
NA	25-09-2017	1.9	IBM Business Process Manager 7.5, 8.0, and 8.5 temporarily stores files in a temporary folder during offline installs which could be read by a local user within a short timespan. IBM X-Force ID: 126461. **CVE ID: CVE-2017-1346**	http://www.ibm.com/support/docview.wss?uid=swg22004654	A-IBM-BUSIN-011017/86
Security Identity Manager					
NA	25-09-2017	2.1	IBM Security Identity Manager	http://www.ib	A-IBM-

			Adapters 6.0 and 7.0 stores user credentials in plain in clear text which can be read by a local user. IBM X-Force ID: 126801. **CVE ID: CVE-2017-1362**	m.com/support/docview.wss?uid=swg22007381	SECUR-011017/87
Curam Social Program Management					
XSS	19-09-2017	3.5	Cross-site scripting (XSS) vulnerability in IBM Curam Social Program Management 6.0 SP2, 6.0.4, and 6.0.5 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors. IBM X-Force ID: 98568. **CVE ID: CVE-2014-6191**	http://www-01.ibm.com/support/docview.wss?uid=swg21698430	A-IBM-CURAM-011017/88
Business Process Manager					
XSS	25-09-2017	3.5	IBM Business Process Manager 8.5.7 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 127477. **CVE ID: CVE-2017-1424**	http://www.ibm.com/support/docview.wss?uid=swg22005112	A-IBM-BUSIN-011017/89
XSS	2017-09-26	3.5	IBM Business Process Manager 7.5, 8.0, and 8.5 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 130410. **CVE ID: CVE-2017-1531**	http://www.ibm.com/support/docview.wss?uid=swg22007354	A-IBM-BUSIN-011017/90
XSS	2017-09-26	3.5	IBM Business Process Manager 7.5, 8.0, and 8.5 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	http://www.ibm.com/support/docview.wss?uid=swg22007351	A-IBM-BUSIN-011017/91

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

			IBM X-Force ID: 130409. **CVE ID: CVE-2017-1530**		
XSS	2017-09-26	3.5	IBM Business Process Manager 8.0.1.1 and 8.5.7 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 127478. **CVE ID: CVE-2017-1425**	http://www.ibm.com/support/docview.wss?uid=swg22006265	A-IBM-BUSIN-011017/92
Api Connect					
NA	25-09-2017	4	IBM API Connect 5.0.0.0 through 5.0.7.2 could allow an authenticated user to generate an API token when not subscribed to the application plan. IBM X-Force ID: 131545. **CVE ID: CVE-2017-1555**	http://www.ibm.com/support/docview.wss?uid=swg22008588	A-IBM-API C-011017/93
Websphere Mq					
DoS	25-09-2017	4	IBM WebSphere MQ 8.0 could allow an authenticated user to cause a premature termination of a client application thread which could potentially cause denial of service. IBM X-Force ID: 123914. **CVE ID: CVE-2017-1235**	http://www.ibm.com/support/docview.wss?uid=swg22005415	A-IBM-WEBSP-011017/94
Api Connect					
NA	25-09-2017	5.8	IBM API Connect 5.0.0.0 through 5.0.7.2 could allow a remote attacker to hijack the clicking action of the victim. By persuading a victim to visit a malicious Web site, a remote attacker could exploit this vulnerability to hijack the victim's click actions and possibly launch further attacks against the victim. IBM X-Force ID: 131291. **CVE ID: CVE-2017-1551**	http://www.ibm.com/support/docview.wss?uid=swg22008372	A-IBM-API C-011017/95
Business Process Manager					

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

Gain Privileges	2017-09-26	6.5	IBM Business Process Manager 7.5, 8.0, and 8.5 is vulnerable to privilege escalation by not properly distinguishing internal group memberships from user registry group memberships. By manipulating LDAP group membership an attack might gain privileged access. IBM X-Force ID: 130807. **CVE ID: CVE-2017-1539**	http://www.ibm.com/support/docview.wss?uid=swg22007451	A-IBM-BUSIN-011017/96
Security Identity Manager					
XSS CSRF	18-09-2017	6.8	Cross-site request forgery (CSRF) vulnerability in IBM Security Identity Manager 5.1, 6.0, and 7.0 allows remote attackers to hijack the authentication of users for requests that can cause cross-site scripting attacks, web cache poisoning, or other unspecified impacts via unknown vectors. **CVE ID: CVE-2014-6106**	https://www-01.ibm.com/support/docview.wss?uid=swg21698020	A-IBM-SECUR-011017/97
Security Siteprotector System					
Gain Privileges	20-09-2017	6.9	IBM Security SiteProtector System 3.0, 3.1, and 3.1.1 allows local users to gain privileges. **CVE ID: CVE-2015-0162**	https://www-01.ibm.com/support/docview.wss?uid=swg21700012	A-IBM-SECUR-011017/98
Business Process Manager					
NA	2017-09-26	7.5	IBM Business Process Manager 7.5, 8.0, and 8.5 is vulnerable to a XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 130156. **CVE ID: CVE-2017-1527**	http://www.ibm.com/support/docview.wss?uid=swg22007346	A-IBM-BUSIN-011017/99
Imagemagick					
Imagemagick					
Overflow	17-09-2017	4.3	ImageMagick 7.0.6-6 has a memory leak in ReadMATImage in coders/mat.c. **CVE ID: CVE-2017-**	https://github.com/ImageMagick/ImageMa	A-IMA-IMAGE-011017

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

			14533	gick/issues/648	/100
DoS	17-09-2017	4.3	The TIFFSetProfiles function in coders/tiff.c in ImageMagick 7.0.6 has incorrect expectations about whether LibTIFF TIFFGetField return values imply that data validation has occurred, which allows remote attackers to cause a denial of service (use-after-free after an invalid call to TIFFSetField, and application crash) via a crafted file. **CVE ID: CVE-2017-14528**	NA	A-IMA-IMAGE-011017/101
DoS	17-09-2017	4.3	DrawGetStrokeDashArray in wand/drawing-wand.c in ImageMagick 7.0.7-1 mishandles certain NULL arrays, which allows attackers to perform Denial of Service (NULL pointer dereference and application crash in AcquireQuantumMemory within MagickCore/memory.c) by providing a crafted Image File as input. **CVE ID: CVE-2017-14505**	https://github.com/ImageMagick/ImageMagick/issues/716	A-IMA-IMAGE-011017/102
DoS	25-09-2017	4.3	The ReadCAPTIONImage function in coders/caption.c in ImageMagick 7.0.7-3 allows remote attackers to cause a denial of service (infinite loop) via a crafted font file. **CVE ID: CVE-2017-14741**	https://github.com/ImageMagick/ImageMagick/issues/771	A-IMA-IMAGE-011017/103
DoS	25-09-2017	5	The AcquireResampleFilterThreadSet function in magick/resample-private.h in ImageMagick 7.0.7-4 mishandles failed memory allocation, which allows remote attackers to cause a denial of service (NULL Pointer Dereference in DistortImage in MagickCore/distort.c, and application crash) via unspecified vectors. **CVE ID: CVE-2017-14739**	https://github.com/ImageMagick/ImageMagick/issues/780	A-IMA-IMAGE-011017/104
NA	20-09-2017	5.8	In ImageMagick 7.0.7-4 Q16, an out of bounds read flaw related to	https://github.com/ImageMa	A-IMA-IMAGE-

			ReadTIFFImage has been reported in coders/tiff.c. An attacker could possibly exploit this flaw to disclose potentially sensitive memory or cause an application crash. **CVE ID: CVE-2017-14607**	gick/ImageMagick/issues/765	011017/105
DoS Overflow	21-09-2017	6.8	GetNextToken in MagickCore/token.c in ImageMagick 7.0.6 allows remote attackers to cause a denial of service (heap-based buffer overflow and application crash) or possibly have unspecified other impact via a crafted SVG document, a different vulnerability than CVE-2017-10928. **CVE ID: CVE-2017-14682**	https://www.imagemagick.org/discourse-server/viewtopic.php?f=3&t=32726	A-IMA-IMAGE-011017/106
NA	17-09-2017	7.1	ImageMagick 7.0.7-0 has a memory exhaustion issue in ReadSUNImage in coders/sun.c. **CVE ID: CVE-2017-14531**	https://github.com/ImageMagick/ImageMagick/issues/718	A-IMA-IMAGE-011017/107
DoS	21-09-2017	7.1	In ImageMagick 7.0.7-4 Q16, a memory leak vulnerability was found in the function ReadVIPSImage in coders/vips.c, which allows attackers to cause a denial of service (memory consumption in ResizeMagickMemory in MagickCore/memory.c) via a crafted file. **CVE ID: CVE-2017-14684**	https://github.com/ImageMagick/ImageMagick/issues/770	A-IMA-IMAGE-011017/108
NA	17-09-2017	7.5	ImageMagick 7.0.7-0 has a NULL Pointer Dereference in TIFFIgnoreTags in coders/tiff.c. **CVE ID: CVE-2017-14532**	https://github.com/ImageMagick/ImageMagick/issues/719	A-IMA-IMAGE-011017/109
NA	21-09-2017	7.5	ImageMagick 7.0.7-0 Q16 has a NULL Pointer Dereference vulnerability in the function sixel_decode in coders/sixel.c. **CVE ID: CVE-2017-14626**	https://github.com/ImageMagick/ImageMagick/issues/720	A-IMA-IMAGE-011017/110

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	21-09-2017	7.5	ImageMagick 7.0.7-0 Q16 has a NULL Pointer Dereference vulnerability in the function sixel_output_create in coders/sixel.c. **CVE ID: CVE-2017-14625**	https://github.com/ImageMagick/ImageMagick/issues/721	A-IMA-IMAGE-011017/111
NA	21-09-2017	7.5	ImageMagick 7.0.7-0 Q16 has a NULL Pointer Dereference vulnerability in the function PostscriptDelegateMessage in coders/ps.c. **CVE ID: CVE-2017-14624**	https://github.com/ImageMagick/ImageMagick/issues/722	A-IMA-IMAGE-011017/112
Ipython					
Ipython					
XSS	20-09-2017	4.3	Cross-site scripting (XSS) vulnerability in IPython before 3.2 allows remote attackers to inject arbitrary web script or HTML via vectors involving JSON error messages and the /api/notebooks path. **CVE ID: CVE-2015-4707**	https://bugzilla.redhat.com/show_bug.cgi?id=1235688	A-IPY-IPYTH-011017/113
XSS	21-09-2017	4.3	Cross-site scripting (XSS) vulnerability in IPython 3.x before 3.2 allows remote attackers to inject arbitrary web script or HTML via vectors involving JSON error messages and the /api/contents path. **CVE ID: CVE-2015-4706**	https://ipython.org/ipython-doc/3/whatsnew/version3.html	A-IPY-IPYTH-011017/114
Irfanview					
Irfanview					
DoS Overflow	18-09-2017	4.6	IrfanView 4.44 - 32bit allows attackers to cause a denial of service or possibly have unspecified other impact via a crafted .ani file, related to "Data from Faulting Address controls Branch Selection starting at ntdll_77130000!RtlpCoalesceFreeBlocks+0x00000000000004b4." **CVE ID: CVE-2017-14578**	https://github.com/wlinzi/security_advisories/tree/master/CVE-2017-14578	A-IRF-IRFAN-011017/115
DoS Overflow	18-09-2017	4.6	IrfanView 4.44 - 32bit allows attackers to cause a denial of	https://github.com/wlinzi/se	A-IRF-IRFAN-

			service or possibly have unspecified other impact via a crafted .svg file, related to "Data from Faulting Address controls Branch Selection starting at CADIMAGE+0x000000000001f23e. " **CVE ID: CVE-2017-14540**	curity_advisories/tree/master/CVE-2017-14540	011017/116
DoS Overflow	18-09-2017	4.6	IrfanView 4.44 - 32bit allows attackers to cause a denial of service or possibly have unspecified other impact via a crafted .svg file, related to "Data from Faulting Address controls Branch Selection starting at image00000000_00400000+0x000000000011d767." **CVE ID: CVE-2017-14539**	https://github.com/wlinzi/security_advisories/tree/master/CVE-2017-14539	A-IRF-IRFAN-011017/117
DoS Overflow	22-09-2017	4.6	IrfanView 4.44 - 32bit allows attackers to cause a denial of service or possibly have unspecified other impact via a crafted .djvu file, related to "Data from Faulting Address controls Branch Selection starting at DJVU!GetPlugInInfo+0x000000000001c613." **CVE ID: CVE-2017-14693**	https://github.com/wlinzi/security_advisories/tree/master/CVE-2017-14693	A-IRF-IRFAN-011017/118
Joomla					
Joomla!					
Gain Information	20-09-2017	4.3	In Joomla! before 3.8.0, a logic bug in a SQL query could lead to the disclosure of article intro texts when these articles are in the archived state. **CVE ID: CVE-2017-14595**	https://developer.joomla.org/security-centre/710-20170901-core-information-disclosure	A-JOO-JOOML-011017/119
NA	20-09-2017	5	In Joomla! before 3.8.0, inadequate escaping in the LDAP authentication plugin can result in a disclosure of a username and password. **CVE ID: CVE-2017-14596**	https://developer.joomla.org/security-centre/711-20170902-core-ldap-	A-JOO-JOOML-011017/120

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

				information-disclosure	
NA	20-09-2017	5.8	Open redirect vulnerability in Joomla! CMS 3.0.0 through 3.4.1. **CVE ID: CVE-2015-5608**	https://developer.joomla.org/security-centre/617-20150601-core-open-redirect.html	A-JOO-JOOML-011017/121
Jsoup					
Jsoup					
XSS	25-09-2017	4.3	Cross-site scripting (XSS) vulnerability in jsoup before 1.8.3. **CVE ID: CVE-2015-6748**	https://bugzilla.redhat.com/show_bug.cgi?id=1258310	A-JSO-JSOUP-011017/122
Kallithea					
Kallithea					
XSS	19-09-2017	3.5	Multiple cross-site scripting (XSS) vulnerabilities in the administration pages in Kallithea before 0.2.1 allow remote attackers to inject arbitrary web script or HTML via the (1) first name or (2) last name user details, or the (3) repository, (4) repository group, or (5) user group description. **CVE ID:CVE-2015-1864**	https://kallithea-scm.org/security/cve-2015-1864.html	A-KAL-KALLI-011017/123
CSRF	21-09-2017	6.8	Cross-site request forgery (CSRF) vulnerability in Kallithea before 0.2. **CVE ID: CVE-2015-0276**	https://kallithea-scm.org/security/cve-2015-0276.html	A-KAL-KALLI-011017/124
Kaltura					
Kaltura Server					
XSS	19-09-2017	4.3	Multiple cross-site scripting (XSS) vulnerabilities in Kaltura before 13.2.0 allow remote attackers to inject arbitrary web script or HTML via the (1) partnerId or (2) playerVersion parameter to server/admin_console/web/tools/bigRedButton.php; the (3)	https://github.com/kaltura/server/pull/6003/commits/7e00a578d6ba748f6d3bdc255a40a4a0a594e6f9	A-KAL-KALTU-011017/125

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

			partnerId, (4) playerVersion, (5) secret, (6) entryId, (7) adminUiConfId, or (8) uiConfId parameter to server/admin_console/web/tools/bigRedButtonPtsPoc.php; the (9) streamUsername, (10) streamPassword, (11) streamRemoteId, (12) streamRemoteBackupId, or (13) entryId parameter to server/admin_console/web/tools/AkamaiBroadcaster.php; the (14) entryId parameter to server/admin_console/web/tools/XmlJWPlayer.php; or the (15) partnerId or (16) playerVersion parameter to server/alpha/web/lib/bigRedButtonPtsPocHlsjs.php. **CVE ID: CVE-2017-14142**		
Execute Code	19-09-2017	6.5	The wiki_decode Developer System Helper function in the admin panel in Kaltura before 13.2.0 allows remote attackers to conduct PHP object injection attacks and execute arbitrary PHP code via a crafted serialized object. **CVE ID: CVE-2017-14141**	https://github.com/kaltura/server/commit/6a6d14328b7a1493e8c47f9565461e5f88be20c9#diff-0770640cc76112cbf77bebc604852682	A-KAL-KALTU-011017/126
Execute Code Bypass	19-09-2017	7.5	The getUserzoneCookie function in Kaltura before 13.2.0 uses a hardcoded cookie secret to validate cookie signatures, which allows remote attackers to bypass an intended protection mechanism and consequently conduct PHP object injection attacks and execute arbitrary PHP code via a crafted userzone cookie. **CVE ID: CVE-2017-14143**	https://github.com/kaltura/server/commit/6a6d14328b7a1493e8c47f9565461e5f88be20c9#diff-0770640cc76112cbf77bebc604852682	A-KAL-KALTU-011017/127
Landesk					

Landesk Management Suite					
File Inclusion	19-09-2017	6.5	The admin interface in Landesk Management Suite 9.6 and earlier allows remote attackers to conduct remote file inclusion attacks involving ASPX pages from third-party sites via the d parameter to (1) ldms/sm_actionfrm.asp or (2) remote/frm_coremainfrm.aspx; or the (3) top parameter to remote/frm_splitfrm.aspx. **CVE ID: CVE-2014-5362**	NA	A-LAN-LANDE-011017/128
Lenovo					
Xclarity Administrator					
NA	22-09-2017	2.1	An attacker who obtains access to the location where the LXCA file system is stored may be able to access credentials of local LXCA accounts in LXCA versions earlier than 1.3.2. **CVE ID: CVE-2017-3763**	https://support.lenovo.com/us/en/product_security/LEN-16333	A-LEN-XCLAR-011017/129
Execute Code	22-09-2017	6.5	Privilege escalation vulnerability in LXCA versions earlier than 1.3.2 where an authenticated user may be able to abuse certain web interface functionality to execute privileged commands within the underlying LXCA operating system. **CVE ID: CVE-2017-3770**	https://support.lenovo.com/us/en/product_security/LEN-16333	A-LEN-XCLAR-011017/130
Libarchive					
Libarchive					
NA	17-09-2017	4.3	libarchive 3.3.2 suffers from an out-of-bounds read within lha_read_data_none() in archive_read_support_format_lha.c when extracting a specially crafted lha archive, related to lha_crc16. **CVE ID: CVE-2017-14503**	NA	A-LIB-LIBAR-011017/131
NA	17-09-2017	4.3	An out-of-bounds read flaw exists in parse_file_info in archive_read_support_format_iso9660.c in libarchive 3.3.2 when	NA	A-LIB-LIBAR-011017/132

			extracting a specially crafted iso9660 iso file, related to archive_read_format_iso9660_read_header. **CVE ID: CVE-2017-14501**		
NA	17-09-2017	5	read_header in archive_read_support_format_rar.c in libarchive 3.3.2 suffers from an off-by-one error for UTF-16 names in RAR archives, leading to an out-of-bounds read in archive_read_format_rar_read_header. **CVE ID: CVE-2017-14502**	NA	A-LIB-LIBAR-011017/133
Libbpg Project					
Libbpg					
DoS Overflow	25-09-2017	6.8	The build_msps function in libbpg.c in libbpg 0.9.7 allows remote attackers to cause a denial of service (heap-based buffer overflow and application crash) or possibly have unspecified other impact via a crafted BPG file, related to hevc_decode_init1. **CVE ID: CVE-2017-14734**	https://github.com/leonzhao7/vulnerability/blob/master/A%20heap-buffer-overflow%20vulnerability%20in%20hevc_decode_init1%20of%20libbpg.md	A-LIB-LIBBP-011017/134
DoS	27-09-2017	6.8	The hevc_write_frame function in libbpg.c in libbpg 0.9.7 allows remote attackers to cause a denial of service (integer underflow and application crash) or possibly have unspecified other impact via a crafted BPG file, related to improper interaction with copy_CTB_to_hv in hevc_filter.c in libavcodec in FFmpeg and sao_filter_CTB in hevc_filter.c in libavcodec in FFmpeg. **CVE ID: CVE-2017-14796**	https://github.com/leonzhao7/vulnerability/blob/master/An%20integer%20underflow%20vulnerability%20in%20sao_filter_CTB%20of%20libbpg.md	A-LIB-LIBBP-011017/135
DoS	27-09-2017	6.8	The hevc_write_frame function in libbpg.c in libbpg 0.9.7 allows remote attackers to cause a denial of service (out-of-bounds read and	https://github.com/leonzhao7/vulnerability/blob/master	A-LIB-LIBBP-011017/136

			application crash) or possibly have unspecified other impact via a crafted BPG file, related to improper interaction with hls_pcm_sample in hevc.c in libavcodec in FFmpeg and put_pcm_var in hevcdsp_template.c in libavcodec in FFmpeg. **CVE ID: CVE-2017-14795**	/An%20Out-of-Bounds%20Read%20%28DoS%29%20Vulnerability%20in%20hevc.c%20of%20libbpg.md	
Libofx					
DoS Overflow	25-09-2017	4.3	ofx_proc_file in ofx_preproc.cpp in LibOFX 0.9.12 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted file, as demonstrated by an ofxdump call. **CVE ID: CVE-2017-14731**	https://github.com/libofx/libofx/issues/10	A-LIB-LIBOF-011017/137
Libpgf					
Libpgf					
NA	20-09-2017	7.5	Use-after-free vulnerability in Decoder.cpp in libpgf before 6.15.32. **CVE ID: CVE-2015-6673**	NA	A-LIB-LIBPG-011017/138
Libraw					
Libraw					
NA	20-09-2017	6.4	In LibRaw through 0.18.4, an out of bounds read flaw related to kodak_65000_load_raw has been reported in dcraw/dcraw.c and internal/dcraw_common.cpp. An attacker could possibly exploit this flaw to disclose potentially sensitive memory or cause an application crash. **CVE ID: CVE-2017-14608**	https://github.com/LibRaw/LibRaw/commit/d13e8f6d1e987b7491182040a188c16a395f1d21	A-LIB-LIBRA-011017/139
Libsndfile Project					
Libsndfile					
NA	21-09-2017	4.3	In libsndfile 1.0.28, a divide-by-zero error exists in the function double64_init() in double64.c, which may lead to DoS when	https://github.com/erikd/libsndfile/issues/318	A-LIB-LIBSN-011017/140

			playing a crafted audio file. **CVE ID: CVE-2017-14634**		
NA	21-09-2017	5.8	An out of bounds read in the function d2ulaw_array() in ulaw.c of libsndfile 1.0.28 may lead to a remote DoS attack or information disclosure, related to mishandling of the NAN and INFINITY floating-point values. **CVE ID: CVE-2017-14246**	https://github.com/erikd/libsndfile/issues/317	A-LIB-LIBSN-011017/141
NA	21-09-2017	5.8	An out of bounds read in the function d2alaw_array() in alaw.c of libsndfile 1.0.28 may lead to a remote DoS attack or information disclosure, related to mishandling of the NAN and INFINITY floating-point values. **CVE ID: CVE-2017-14245**	https://github.com/erikd/libsndfile/issues/317	A-LIB-LIBSN-011017/142
Litespeedtech					
Open Litespeed					
NA	20-09-2017	5	Use-after-free vulnerability in Open Litespeed before 1.3.10. **CVE ID: CVE-2015-3890**	http://www.security-assessment.com/files/documents/advisory/Open%20Litespeed%20Use%20After%20Free%20Vulnerability.pdf	A-LIT-OPEN-011017/143
Magento					
E-commerce					
XSS	20-09-2017	4.3	Cross-site scripting (XSS) vulnerability in Magento E-Commerce Platform 1.9.0.1. **CVE ID: CVE-2014-9758**	NA	A-MAG-E-COM-011017/144
Metinfo					
Metinfo					
Dir. Trav.	17-09-2017	5	Directory traversal vulnerability in MetInfo 5.3.17 allows remote attackers to read information from any ini format file via the	https://github.com/phantom0301/vulns/blob/master/Me	A-MET-METIN-011017/145

			f_filename parameter in a fingerprintdo action to admin/app/physical /physical.php. **CVE ID: CVE-2017-14513**	tinfo2.md	
Microfocus					
Visibroker					
DoS Overflow	21-09-2017	5	An integer overflow (CWE-190) potentially causing an out-of-bounds read (CWE-125) vulnerability in Micro Focus VisiBroker 8.5 can lead to a denial of service. **CVE ID: CVE-2017-9281**	https://community.microfocus.com/microfocus/corba/visibroker_-_world_class_middleware/w/knowledge_base/29171/visibroker-8-5-service-pack-4-hotfix-3-security-fixes	A-MIC-VISIB-011017/146
NA	21-09-2017	7.5	An out-of-bounds read (CWE-125) vulnerability exists in Micro Focus VisiBroker 8.5. The feasibility of leveraging this vulnerability for further attacks was not assessed. **CVE ID: CVE-2017-9283**	https://community.microfocus.com/microfocus/corba/visibroker_-_world_class_middleware/w/knowledge_base/29171/visibroker-8-5-service-pack-4-hotfix-3-security-fixes	A-MIC-VISIB-011017/147
Overflow	21-09-2017	7.5	An integer overflow (CWE-190) led to an out-of-bounds write (CWE-787) on a heap-allocated area, leading to heap corruption in Micro Focus VisiBroker 8.5. The feasibility of leveraging this vulnerability for further attacks was not assessed. **CVE ID: CVE-2017-9282**	https://community.microfocus.com/microfocus/corba/visibroker_-_world_class_middleware/w/knowledge_base/29171/visibroker-8-5-service-pack-	A-MIC-VISIB-011017/148

				4-hotfix-3-security-fixes	
Mirasvit					
Helpdesk Mx					
XSS	21-09-2017	3.5	Multiple cross-site scripting (XSS) vulnerabilities in the administrative interface in Mirasvit Helpdesk MX before 1.5.3 allow remote attackers to inject arbitrary web script or HTML via the (1) customer name or (2) subject in a ticket. **CVE ID:CVE-2017-14321**	https://www.webshield.hu/vulnerabilities-found-webshield.html	A-MIR-HELPD-011017/149
Execute Code	21-09-2017	6	Mirasvit Helpdesk MX before 1.5.3 might allow remote attackers to execute arbitrary code by leveraging failure to filter uploaded files. **CVE ID: CVE-2017-14320**	https://www.webshield.hu/vulnerabilities-found-webshield.html	A-MIR-HELPD-011017/150
Moodle					
Moodle					
Gain Information	18-09-2017	4	In Moodle 3.x, various course reports allow teachers to view details about users in the groups they can't access. **CVE ID: CVE-2017-12157**	https://moodle.org/mod/forum/discuss.php?d=358586	A-MOO-MOODL-011017/151
XSS	18-09-2017	4.3	Moodle 3.x has XSS in the contact form on the "non-respondents" page in non-anonymous feedback. **CVE ID: CVE-2017-12156**	https://moodle.org/mod/forum/discuss.php?d=358585	A-MOO-MOODL-011017/152
Netmechanica					
Netdecision					
Gain Privileges	19-09-2017	4.6	The Winring0x32.sys driver in NetMechanica NetDecision 5.8.2 allows local users to gain privileges via a crafted 0x9C402088 IOCTL call. **CVE ID: CVE-2017-14311**	https://www.exploit-db.com/exploits/42735/	A-NET-NETDE-011017/153
Netsweeper					
Netsweeper					
Gain Information	19-09-2017	5	Netsweeper before 3.1.10, 4.0.x before 4.0.9, and 4.1.x before 4.1.2 allows remote attackers to obtain sensitive information by making a	http://packetstormsecurity.com/files/133034/Netsweepe	A-NET-NETSW-011017/154

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

			request that redirects to the deny page. **CVE ID: CVE-2014-9616**	r-Bypass-XSS-Redirection-SQL-Injection-Execution.html	
Bypass	19-09-2017	5	Netsweeper before 3.1.10, 4.0.x before 4.0.9, and 4.1.x before 4.1.2 allows remote attackers to bypass authentication and remove IP addresses from the quarantine via the ip parameter to webadmin/user/quarantine _disable.php. **CVE ID: CVE-2014-9610**	NA	A-NET-NETSW-011017/155
Execute Code	19-09-2017	6.5	Unrestricted file upload vulnerability in webadmin/ajaxfilemanager/ajaxfilemanager.php in Netsweeper before 3.1.10, 4.0.x before 4.0.9, and 4.1.x before 4.1.2 allows remote authenticated users with admin privileges on the Cloud Manager web console to execute arbitrary PHP code by uploading a file with a double extension, then accessing it via a direct request to the file in webadmin/deny/images/, as demonstrated by secuid0.php.gif. **CVE ID: CVE-2014-9619**	NA	A-NET-NETSW-011017/156
Bypass	19-09-2017	7.5	The Client Filter Admin portal in Netsweeper before 3.1.10, 4.0.x before 4.0.9, and 4.1.x before 4.1.2 allows remote attackers to bypass authentication and subsequently create arbitrary profiles via a showdeny action to the default URL. **CVE ID: CVE-2014-9618**	NA	A-NET-NETSW-011017/157
Bypass	19-09-2017	7.5	Netsweeper before 4.0.5 allows remote attackers to bypass authentication and create arbitrary accounts and policies via a request to webadmin/nslam/index.php. **CVE ID: CVE-2014-9611**	NA	A-NET-NETSW-011017/158

Newsbeuter					
Newsbeuter					
Execute Code	17-09-2017	6.8	Improper Neutralization of Special Elements used in an OS Command in the podcast playback function of Podbeuter in Newsbeuter 0.3 through 2.9 allows remote attackers to perform user-assisted code execution by crafting an RSS item with a media enclosure (i.e., a podcast file) that includes shell metacharacters in its filename, related to pb_controller.cpp and queueloader.cpp, a different vulnerability than CVE-2017-12904. **CVE ID: CVE-2017-14500**	NA	A-NEW-NEWSB-011017/159
Nexusphp Project					
Nexusphp					
XSS	18-09-2017	4.3	Cross Site Scripting (XSS) exists in NexusPHP 1.5.beta5.20120707 via the PATH_INFO to location.php, related to PHP_SELF. **CVE ID: CVE-2017-14534**	https://raw.githubusercontent.com/yangchonghui2017/cve/master/2.txt	A-NEX-NEXUS-011017/160
Sql	17-09-2017	7.5	NexusPHP 1.5.beta5.20120707 has SQL Injection in forummanage.php via the sort parameter in an editforum action, a different vulnerability than CVE-2017-12981. **CVE ID: CVE-2017-14512**	https://github.com/rezhish/NexusPHP/blob/master/nexusphp.md	A-NEX-NEXUS-011017/161
Nodebb					
Nodebb					
XSS	21-09-2017	4.3	Multiple cross-site scripting (XSS) vulnerabilities in NodeBB before 0.7 allow remote attackers to inject arbitrary web script or HTML via vectors related to (1) javascript: or (2) data: URLs. **CVE ID: CVE-2015-3296**	https://github.com/julianlam/nodebb-plugin-markdown/commit/ab7f2684750882f7baefbfa31db8d5aac71e6ec3	A-NOD-NODEB-011017/162
Nvidia					
Gpu Driver					

DoS	22-09-2017	4.9	NVIDIA Windows GPU Display Driver contains a vulnerability in the kernel mode layer handler for DxgkDdiCreateAllocation where untrusted user input is used as a divisor without validation while processing block linear information which may lead to a potential divide by zero and denial of service. **CVE ID: CVE-2017-6271**	http://nvidia.custhelp.com/app/answers/detail/a_id/4544	A-NVI-GPU D-011017/163
DoS	22-09-2017	4.9	NVIDIA Windows GPU Display Driver contains a vulnerability in the kernel mode layer handler for DxgkDdiCreate Allocation where untrusted user input is used as a divisor without validation during a calculation which may lead to a potential divide by zero and denial of service. **CVE ID: CVE-2017-6270**	http://nvidia.custhelp.com/app/answers/detail/a_id/4544	A-NVI-GPU D-011017/164
DoS Overflow	22-09-2017	4.9	NVIDIA GPU Display Driver contains a vulnerability in the kernel mode layer handler where an incorrect initialization of internal objects can cause an infinite loop which may lead to a denial of service. **CVE ID: CVE-2017-6267**	http://nvidia.custhelp.com/app/answers/detail/a_id/4544	A-NVI-GPU D-011017/165
DoS	22-09-2017	4.9	NVIDIA GPU Display Driver contains a vulnerability in the kernel mode layer handler where improper access controls could allow unprivileged users to cause a denial of service. **CVE-2017-6266**	http://nvidia.custhelp.com/app/answers/detail/a_id/4544	A-NVI-GPU D-011017/166
DoS	22-09-2017	7.2	NVIDIA Windows GPU Display Driver contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape where a value passed from a user to the driver is not correctly validated and used as the index to an array which may	http://nvidia.custhelp.com/app/answers/detail/a_id/4544	A-NVI-GPU D-011017/167

			lead to denial of service or possible escalation of privileges. **CVE ID: CVE-2017-6277**		
DoS	22-09-2017	7.2	NVIDIA GPU Display Driver contains a vulnerability in the kernel mode layer handler where a value passed from a user to the driver is not correctly validated and used as the index to an array which may lead to a denial of service or possible escalation of privileges. **CVE ID: CVE-2017-6272**	http://nvidia.custhelp.com/app/answers/detail/a_id/4544	A-NVI-GPU D-011017/168
DoS	22-09-2017	7.2	NVIDIA Windows GPU Display Driver contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape where a pointer passed from a user to the driver is used without validation which may lead to denial of service or possible escalation of privileges. **CVE ID: CVE-2017-6269**	http://nvidia.custhelp.com/app/answers/detail/a_id/4544	A-NVI-GPU D-011017/169
DoS	22-09-2017	7.2	NVIDIA Windows GPU Display Driver contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape where a value passed from a user to the driver is not correctly validated and used as the index to an array which may lead to denial of service or possible escalation of privileges. **CVE ID: CVE-2017-6268**	http://nvidia.custhelp.com/app/answers/detail/a_id/4544	A-NVI-GPU D-011017/170
Openwebif Project					
Openwebif					
Execute Code	17-09-2017	6.8	OpenWebif 1.2.5 allows remote code execution via a URL to the CallOPKG function in the IpkgController class in plugin/controllers/ipkg.py, when the URL refers to an attacker-controlled web site with a Trojan	NA	A-OPE-OPENW-011017/171

			horse package. This has security implications in cases where untrusted users can trigger CallOPKG calls, and these users can enter an arbitrary URL in an input field, even though that input field was only intended for a package name. This threat model may be relevant in the latest versions of third-party products that bundle OpenWebif, i.e., set-top box products. The issue of Trojan horse packages does NOT have security implications in cases where the attacker has full OpenWebif access. **CVE ID: CVE-2017-9333**		
Otrs					
Otrs					
Gain Privileges	21-09-2017	6.5	In Open Ticket Request System (OTRS) 3.3.x before 3.3.18, 4.x before 4.0.25, and 5.x before 5.0.23, remote authenticated users can leverage statistics-write permissions to gain privileges via code injection. **CVE ID: CVE-2017-14635**	https://www.otrs.com/security-advisory-2017-04-security-update-otrs-versions/	A-OTR-OTRS-011017/172
Perl					
Perl					
DoS Overflow	19-09-2017	5	Heap-based buffer overflow in the S_regatom function in regcomp.c in Perl 5 before 5.24.3-RC1 and 5.26.x before 5.26.1-RC1 allows remote attackers to cause a denial of service (out-of-bounds write) via a regular expression with a '\N{}' escape and the case-insensitive modifier. **CVE ID: CVE-2017-12837**	https://perl5.git.perl.org/perl.git/log/refs/tags/v5.26.1-RC1	A-PER-PERL-011017/173
DoS Overflow	19-09-2017	6.4	Buffer overflow in the S_grok_bslash_N function in regcomp.c in Perl 5 before 5.24.3-RC1 and 5.26.x before 5.26.1-RC1	https://perl5.git.perl.org/perl.git/log/refs/tags/v5.26.1-	A-PER-PERL-011017/174

			allows remote attackers to disclose sensitive information or cause a denial of service (application crash) via a crafted regular expression with an invalid '\N{U+...}' escape. **CVE ID: CVE-2017-12883**	RC1	
Phpbb					
Phpbb					
NA	19-09-2017	5.8	Open redirect vulnerability in phpBB before 3.0.14 and 3.1.x before 3.1.4 allows remote attackers to redirect users of Google Chrome to arbitrary web sites and conduct phishing attacks via unspecified vectors. **CVE ID: CVE-2015-3880**	https://www.phpbb.com/community/viewtopic.php?f=14&t=2313941	A-PHP-PHPBB-011017/175
Phpmyfaq					
Phpmyfaq					
XSS	20-09-2017	3.5	Cross-site scripting (XSS) vulnerability in inc/PMF/Faq.php in phpMyFAQ through 2.9.8 allows remote attackers to inject arbitrary web script or HTML via the Questions field in an "Add New FAQ" action. **CVE ID: CVE-2017-14618**	NA	A-PHP-PHPMY-011017/176
XSS	20-09-2017	4.3	Cross-site scripting (XSS) vulnerability in phpMyFAQ through 2.9.8 allows remote attackers to inject arbitrary web script or HTML via the "Title of your FAQ" field in the Configuration Module. **CVE ID: CVE-2017-14619**	https://github.com/thorsten/phpMyFAQ/commit/30b0025e19bd95ba28f4eff4d259671e7bb6bb86	A-PHP-PHPMY-011017/177
Plone					
Plone					
XSS	25-09-2017	4.3	Cross-site scripting (XSS) vulnerability in Plone 3.3.0 through 3.3.6, 4.0.0 through 4.0.10, 4.1.0 through 4.1.6, 4.2.0 through 4.2.7, 4.3.x before 4.3.7, and 5.0rc1. **CVE ID: CVE-2015-7316**	https://plone.org/security/hotfix/20150910/non-persistent-xss-in-plone	A-PLO-PLONE-011017/178

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	25-09-2017	4.3	Plone 3.3.0 through 3.3.6, 4.0.0 through 4.0.10, 4.1.0 through 4.1.6, 4.2.0 through 4.2.7, 4.3.0 through 4.3.6, and 5.0rc1 allows remote attackers to add a new member to a Plone site with registration enabled, without acknowledgment of site administrator. **CVE ID: CVE-2015-7315**	https://plone.org/security/hotfix/20150910/anonymous-is-able-to-create-plone-members	A-PLO-PLONE-011017/179
NA	25-09-2017	5	Plone 3.3.0 through 3.3.6 allows remote attackers to inject headers into HTTP responses. **CVE ID: CVE-2015-7318**	https://plone.org/security/hotfix/20150910/header-injection	A-PLO-PLONE-011017/180
Polycom					
Realpresence Resource Manager					
Gain Information	19-09-2017	4	Polycom RealPresence Resource Manager (aka RPRM) before 8.4 allows remote authenticated users to obtain the installation path via an HTTP POST request to PlcmRmWeb/JConfigManager. **CVE ID: CVE-2015-4682**	https://support.polycom.com/global/documents/support/documentation/Security_Center_Post_for_RPRM_CVEs.pdf	A-POL-REALP-011017/181
Gain Privileges	19-09-2017	4.4	Polycom RealPresence Resource Manager (aka RPRM) before 8.4 allows local users with access to the plcm account to gain privileges via a script in /var/polycom/cma/upgrade/scripts, related to a sudo misconfiguration. **CVE ID: CVE-2015-4685**	https://support.polycom.com/global/documents/support/documentation/Security_Center_Post_for_RPRM_CVEs.pdf	A-POL-REALP-011017/182
Dir. Trav.	19-09-2017	5.5	Multiple directory traversal vulnerabilities in Polycom RealPresence Resource Manager (aka RPRM) before 8.4 allow (1) remote authenticated users to read arbitrary files via a .. (dot dot) in the Modifier parameter to PlcmRmWeb/FileDownload; or remote authenticated	https://support.polycom.com/global/documents/support/documentation/Security_Center_Post_for_RPRM_CVEs.pdf	A-POL-REALP-011017/183

			administrators to upload arbitrary files via the (2) Filename or (3) SE_FNAME parameter to PlcmRmWeb/FileUpload or to read and remove arbitrary files via the (4) filePathName parameter in an importSipUriReservations SOAP request to PlcmRmWeb/JUserManager. **CVE ID: CVE-2015-4684**		
NA	19-09-2017	7.2	Polycom RealPresence Resource Manager (aka RPRM) before 8.4 allows local users to have unspecified impact via vectors related to weak passwords. **CVE ID: CVE-2015-4681**	https://support.polycom.com/global/documents/support/documentation/Security_Center_Post_for_RPRM_CVEs.pdf	A-POL-REALP-011017/184
Gain Privileges Gain Information	19-09-2017	7.5	Polycom RealPresence Resource Manager (aka RPRM) before 8.4 allows attackers to obtain sensitive information and potentially gain privileges by leveraging use of session identifiers as parameters with HTTP GET requests. **CVE ID: CVE-2015-4683**	https://support.polycom.com/global/documents/support/documentation/Security_Center_Post_for_RPRM_CVEs.pdf	A-POL-REALP-011017/185
Pragyan Cms Project					
Pragyan Cms					
Sql	19-09-2017	4	Pragyan CMS v3.0 is vulnerable to a Boolean-based SQL injection in cms/admin.lib.php via $_GET['forwhat'], resulting in Information Disclosure. **CVE ID: CVE-2017-14601**	https://github.com/delta/pragyan/issues/228	A-PRA-PRAGY-011017/186
Sql	19-09-2017	4	Pragyan CMS v3.0 is vulnerable to an Error-Based SQL injection in cms/admin.lib.php via $_GET['del_black'], resulting in Information Disclosure. **CVE ID: CVE-2017-14600**	https://github.com/delta/pragyan/issues/228	A-PRA-PRAGY-011017/187

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

Proxychains-ng Project					
Proxychains-ng					
Gain Privileges	21-09-2017	7.2	Untrusted search path vulnerability in ProxyChains-NG before 4.9 allows local users to gain privileges via a Trojan horse libproxychains4.so library in the current working directory, which is referenced in the LD_PRELOAD path. **CVE ID: CVE-2015-3887**	https://bugzilla.redhat.com/show_bug.cgi?id=1147013	A-PRO-PROXY-011017/188
Pydio					
Pydio					
XSS	19-09-2017	4.3	Multiple cross-site scripting (XSS) vulnerabilities in Pydio (formerly AjaXplorer) before 6.0.7 allow remote attackers to inject arbitrary web script or HTML via unspecified vectors, aka "Pydio XSS Vulnerabilities." **CVE ID: CVE-2015-3432**	https://pydio.com/en/community/releases/pydio-core/pydio-607-security-release	A-PYD-PYDIO-011017/189
Execute Code	19-09-2017	10	Pydio (formerly AjaXplorer) before 6.0.7 allows remote attackers to execute arbitrary commands via unspecified vectors, aka "Pydio OS Command Injection Vulnerabilities." **CVE ID:CVE-2015-3431**	https://pydio.com/en/community/releases/pydio-core/pydio-607-security-release	A-PYD-PYDIO-011017/190
Redhat					
Jboss Enterprise Application Platform					
Gain Information	19-09-2017	4.3	AdvancedLdapLodinMogule in Red Hat JBoss Enterprise Application Platform (EAP) before 6.4.1 allows attackers to obtain sensitive information via vectors involving logging the LDAP bind credential password when TRACE logging is enabled. **CVE ID: CVE-2015-1849**	https://github.com/wildfly-security/jboss-negotiation/pull/21	A-RED-JBOSS-011017/191
Feedhenry Enterprise Mobile Application Platform					
NA	20-09-2017	4.3	Reflected file download vulnerability in Red Hat Feedhenry Enterprise Mobile Application	https://bugzilla.redhat.com/show_bug.cgi?i	A-RED-FEEDH-011017

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

			Platform. **CVE ID: CVE-2015-5248**	d=1272326	/192
Edeploy					
Execute Code Gain Information	19-09-2017	7.5	eDeploy makes it easier for remote attackers to execute arbitrary code by leveraging use of HTTP to download files. **CVE ID: CVE-2014-8174**	https://bugzilla.redhat.com/show_bug.cgi?id=1202972	A-RED-EDEPL-011017/193
Ruby-lang					
Ruby					
DoS Overflow	19-09-2017	5	The decode method in the OpenSSL::ASN1 module in Ruby before 2.2.8, 2.3.x before 2.3.5, and 2.4.x through 2.4.1 allows attackers to cause a denial of service (interpreter crash) via a crafted string. **CVE ID: CVE-2017-14033**	https://www.ruby-lang.org/en/news/2017/09/14/ruby-2-3-5-released/	A-RUB-RUBY-011017/194
Execute Code	19-09-2017	9.3	The Basic authentication code in WEBrick library in Ruby before 2.2.8, 2.3.x before 2.3.5, and 2.4.x through 2.4.1 allows remote attackers to inject terminal emulator escape sequences into its log and possibly execute arbitrary commands via a crafted user name. **CVE ID: CVE-2017-10784**	https://www.ruby-lang.org/en/news/2017/09/14/ruby-2-2-8-released/	A-RUB-RUBY-011017/195
Sam2p Project					
Sam2p					
NA	21-09-2017	5	In sam2p 0.49.3, the in_xpm_reader function in in_xpm.cpp has an integer signedness error, leading to a crash when writing to an out-of-bounds array element. **CVE ID: CVE-2017-14629**	https://github.com/pts/sam2p/issues/14	A-SAM-SAM2P-011017/196
Overflow	21-09-2017	7.5	In sam2p 0.49.3, the pcxLoadRaster function in in_pcx.cpp has an integer signedness error leading to a heap-based buffer overflow. **CVE ID:CVE-2017-14631**	https://github.com/pts/sam2p/issues/14	A-SAM-SAM2P-011017/197
Overflow	21-09-2017	7.5	In sam2p 0.49.3, an integer overflow exists in the pcxLoadImage24 function of the file in_pcx.cpp, leading to an invalid	https://github.com/pts/sam2p/issues/14	A-SAM-SAM2P-011017/198

			write operation. **CVE ID:CVE-2017-14630**		
Overflow	21-09-2017	7.5	In sam2p 0.49.3, a heap-based buffer overflow exists in the pcxLoadImage24 function of the file in_pcx.cpp. **CVE ID: CVE-2017-14628**	https://github.com/pts/sam2p/issues/14	A-SAM-SAM2P-011017/199
Overflow	22-09-2017	7.5	In sam2p 0.49.3, there is an invalid read of size 2 in the parse_rgb function in in_xpm.cpp. However, this can also cause a write to an illegal address. **CVE ID: CVE-2017-14637**	https://github.com/pts/sam2p/issues/14	A-SAM-SAM2P-011017/200
Overflow Mem. Corr.	22-09-2017	7.5	Because of an integer overflow in sam2p 0.49.3, a loop executes 0xffffffff times, ending with an invalid read of size 1 in the Image::Indexed::sortPal function in image.cpp. However, this also causes memory corruption because of an attempted write to the invalid d[0xfffffffe] array element. **CVE ID: CVE-2017-14636**	https://github.com/pts/sam2p/issues/14	A-SAM-SAM2P-011017/201
SAP					
E-recruiting					
Bypass	17-09-2017	5	An issue was discovered in SAP E-Recruiting (aka ERECRUIT) 605 through 617. When an external applicant registers to the E-Recruiting application, he/she receives a link by email to confirm access to the provided email address. However, this measure can be bypassed and attackers can register and confirm email addresses that they do not have access to (candidate_hrobject is predictable and corr_act_guid is improperly validated). Furthermore, since an email address can be registered only once, an attacker could prevent other legitimate users from	NA	A-SAP-E-REC-011017/202

			registering. This is SAP Security Note 2507798. **CVE ID: CVE-2017-14511**		
Netweaver					
DoS	19-09-2017	5	The Host Control web service in SAP NetWeaver AS JAVA 7.0 through 7.5 allows remote attackers to cause a denial of service (service crash) via a crafted request, aka SAP Security Note 2389181. **CVE ID: CVE-2017-14581**	https://erpscan.com/advisories/erpscan-17-030-sap-hostcontrol-remote-dos/	A-SAP-NETWE-011017/203
Schneider-electric					
Citect Anywhere;Powerscada Anywhere					
NA	25-09-2017	3.3	A vulnerability exists in Schneider Electric's PowerSCADA Anywhere v1.0 redistributed with PowerSCADA Expert v8.1 and PowerSCADA Expert v8.2 and Citect Anywhere version 1.0 that allows the ability to specify Arbitrary Server Target Nodes in connection requests to the Secure Gateway and Server components. **CVE ID: CVE-2017-7970**	https://www.citect.schneider-electric.com/safety-and-security-central/36-security-notifications/9071-security-notification-citect-anywhere	A-SCH-CITEC-011017/204
NA	25-09-2017	4	A vulnerability exists in Schneider Electric's PowerSCADA Anywhere v1.0 redistributed with PowerSCADA Expert v8.1 and PowerSCADA Expert v8.2 and Citect Anywhere version 1.0 that allows the use of outdated cipher suites and improper verification of peer SSL Certificate. **CVE ID: CVE-2017-7971**	https://www.citect.schneider-electric.com/safety-and-security-central/36-security-notifications/9071-security-notification-citect-anywhere	A-SCH-CITEC-011017/205
U.motion Builder					
DoS	25-09-2017	4.9	A vulnerability exists in Schneider	http://www.sc	A-SCH-

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

			Electric's U.motion Builder software versions 1.2.1 and prior in which the system accepts reboot in session from unauthenticated users, supporting a denial of service condition. **CVE ID: CVE-2017-9959**	hneider-electric.com/en/download/document/SEVD-2017-178-01/	U.MOT-011017/206
Gain Information	25-09-2017	5	An information disclosure vulnerability exists in Schneider Electric's U.motion Builder software versions 1.2.1 and prior in which the system response to error provides more information than should be available to an unauthenticated user. **CVE ID: CVE-2017-9960**	http://www.schneider-electric.com/en/download/document/SEVD-2017-178-01/	A-SCH-U.MOT-011017/207
Citect Anywhere;Powerscada Anywhere					
NA	25-09-2017	5.2	A vulnerability exists in Schneider Electric's PowerSCADA Anywhere v1.0 redistributed with PowerSCADA Expert v8.1 and PowerSCADA Expert v8.2 and Citect Anywhere version 1.0 that allows the ability to escape out of remote PowerSCADA Anywhere applications and launch other processes. **CVE ID: CVE-2017-7972**	https://www.citect.schneider-electric.com/safety-and-security-central/36-security-notifications/9071-security-notification-citect-anywhere	A-SCH-CITEC-011017/208
CSRF	25-09-2017	6.8	A cross-site request forgery vulnerability exists on the Secure Gateway component of Schneider Electric's PowerSCADA Anywhere v1.0 redistributed with PowerSCADA Expert v8.1 and PowerSCADA Expert v8.2 and Citect Anywhere version 1.0 for multiple state-changing requests. This type of attack requires some level of social engineering in order to get a legitimate user to click on or access a malicious link/site	https://www.citect.schneider-electric.com/safety-and-security-central/36-security-notifications/9071-security-notification-citect-anywhere	A-SCH-CITEC-011017/209

			containing the CSRF attack. **CVE ID: CVE-2017-7969**		
U.motion Builder					
Execute Code	25-09-2017	7.2	An improper access control vulnerability exists in Schneider Electric's U.motion Builder software versions 1.2.1 and prior in which an improper handling of the system configuration can allow an attacker to execute arbitrary code under the context of root. **CVE-2017-9958**	http://www.schneider-electric.com/en/download/document/SEVD-2017-178-01/	A-SCH-U.MOT-011017/210
NA	25-09-2017	7.5	A vulnerability exists in Schneider Electric's U.motion Builder software versions 1.2.1 and prior in which the web service contains a hidden system account with a hardcoded password. An attacker can use this information to log into the system with high-privilege credentials. **CVE ID: CVE-2017-9957**	http://www.schneider-electric.com/en/download/document/SEVD-2017-178-01/	A-SCH-U.MOT-011017/211
Bypass	25-09-2017	7.5	An authentication bypass vulnerability exists in Schneider Electric's U.motion Builder software versions 1.2.1 and prior in which the system contains a hard-coded valid session. An attacker can use that session ID as part of the HTTP cookie of a web request, resulting in authentication bypass **CVE ID: CVE-2017-9956**	http://www.schneider-electric.com/en/download/document/SEVD-2017-178-01/	A-SCH-U.MOT-011017/212
Execute Code Dir. Trav.	25-09-2017	7.5	A path traversal information disclosure vulnerability exists in Schneider Electric's U.motion Builder software versions 1.2.1 and prior in which an unauthenticated user can execute arbitrary code and exfiltrate files. **CVE ID: CVE-2017-7974**	http://www.schneider-electric.com/en/download/document/SEVD-2017-178-01/	A-SCH-U.MOT-011017/213
Sql	25-09-2017	7.5	A SQL injection vulnerability exists in Schneider Electric's U.motion Builder software versions 1.2.1 and	http://www.schneider-electric.com/e	A-SCH-U.MOT-011017

			prior in which an unauthenticated user can use calls to various paths allowing performance of arbitrary SQL commands against the underlying database. **CVE ID: CVE-2017-7973**	n/download/document/SEVD-2017-178-01/	/214
Simple Ads Manager Project					
Simple Ads Manager					
Gain Information	20-09-2017	5	WordPress Simple Ads Manager plugin 2.5.94 and 2.5.96 allows remote attackers to obtain sensitive information. **CVE ID: CVE-2015-2826**	NA	A-SIM-SIMPL-011017/215
Stdutility					
Stdu Viewer					
DoS Execute Code Overflow	18-09-2017	4.6	STDU Viewer 1.6.375 allows attackers to execute arbitrary code or cause a denial of service via a crafted .jb2 file, related to a "Read Access Violation on Control Flow starting at STDUJBIG2File!DllGetClassObject+ 0x0000000000005b70." **CVE ID: CVE-2017-14579**	https://github.com/wlinzi/security_advisories/tree/master/CVE-2017-14579	A-STD-STDU -011017/216
DoS Execute Code Overflow	18-09-2017	4.6	STDU Viewer 1.6.375 allows attackers to execute arbitrary code or cause a denial of service via a crafted .xps file, related to a "Read Access Violation on Control Flow starting at Unknown Symbol @ 0x0000000003aa7cef called from Unknown Symbol @ 0x0000000004aa024d." **CVE ID: CVE-2017-14577**	https://github.com/wlinzi/security_advisories/tree/master/CVE-2017-14577	A-STD-STDU -011017/217
DoS Overflow	18-09-2017	4.6	STDU Viewer 1.6.375 allows attackers to cause a denial of service or possibly have unspecified other impact via a crafted .xps file, related to a "Possible Stack Corruption starting at Unknown Symbol @ 0x00000000049f0281."	https://github.com/wlinzi/security_advisories/tree/master/CVE-2017-14576	A-STD-STDU -011017/218

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

			CVE ID: CVE-2017-14576		
DoS Execute Code Overflow	18-09-2017	4.6	STDU Viewer 1.6.375 allows attackers to execute arbitrary code or cause a denial of service via a crafted .xps file, related to an "Illegal Instruction Violation starting at Unknown Symbol @ 0x0000000002d8024c called from STDUXPSFile!DllUnregisterServer+ 0x000000000002566c." **CVE ID: CVE-2017-14575**	https://github.com/wlinzi/security_advisories/tree/master/CVE-2017-14575	A-STD-STDU - 011017 /219
DoS Execute Code Overflow	18-09-2017	4.6	STDU Viewer 1.6.375 allows attackers to execute arbitrary code or cause a denial of service via a crafted .xps file, related to a "User Mode Write AV starting at Unknown Symbol @ 0x0000000004940490." **CVE ID: CVE-2017-14574**	https://github.com/wlinzi/security_advisories/tree/master/CVE-2017-14574	A-STD-STDU - 011017 /220
DoS Execute Code Overflow	18-09-2017	4.6	STDU Viewer 1.6.375 allows attackers to execute arbitrary code or cause a denial of service via a crafted .xps file, related to an "Illegal Instruction Violation starting at Unknown Symbol @ 0x00000000030c024c called from STDUXPSFile!DllUnregisterServer+ 0x000000000002566a." **CVE ID: CVE-2017-14573**	https://github.com/wlinzi/security_advisories/tree/master/CVE-2017-14573	A-STD-STDU - 011017 /221
DoS Execute Code Overflow	18-09-2017	4.6	STDU Viewer 1.6.375 allows attackers to execute arbitrary code or cause a denial of service via a crafted .xps file, related to a "User Mode Write AV starting at Unknown Symbol @ 0x000000000479049b called from Unknown Symbol @ 0x000000000d89645b." **CVE ID: CVE-2017-14572**	https://github.com/wlinzi/security_advisories/tree/master/CVE-2017-14572	A-STD-STDU - 011017 /222
DoS Execute Code Overflow	18-09-2017	4.6	STDU Viewer 1.6.375 allows attackers to execute arbitrary code or cause a denial of service via a crafted .xps file, related to an	https://github.com/wlinzi/security_advisories/tree/maste	A-STD-STDU - 011017 /223

			"Illegal Instruction Violation starting at Unknown Symbol @ 0x00000000049c024c called from STDUXPSFile!DllUnregisterServer+ 0x0000000000025706." **CVE ID: CVE-2017-14571**	r/CVE-2017-14571	
DoS Execute Code Overflow	18-09-2017	4.6	STDU Viewer 1.6.375 allows attackers to execute arbitrary code or cause a denial of service via a crafted .xps file, related to a "User Mode Write AV near NULL starting at wow64!Wow64LdrpInitialize+0x0 0000000000008e1." **CVE ID: CVE-2017-14570**	https://github.com/wlinzi/security_advisories/tree/master/CVE-2017-14570	A-STD-STDU - 011017 /224
DoS Overflow	18-09-2017	4.6	STDU Viewer 1.6.375 allows attackers to cause a denial of service or possibly have unspecified other impact via a crafted .xps file, related to a "Read Access Violation starting at STDUXPSFile!DllUnregisterServer+ 0x0000000000005bd5." **CVE ID: CVE-2017-14569**	https://github.com/wlinzi/security_advisories/tree/master/CVE-2017-14569	A-STD-STDU - 011017 /225
DoS Execute Code Overflow	18-09-2017	4.6	STDU Viewer 1.6.375 allows attackers to execute arbitrary code or cause a denial of service via a crafted .xps file, related to an "Illegal Instruction Violation starting at Unknown Symbol @ 0x000000000297024c called from STDUXPSFile!DllUnregisterServer+ 0x0000000000025630." **CVE ID: CVE-2017-14568**	https://github.com/wlinzi/security_advisories/tree/master/CVE-2017-14568	A-STD-STDU - 011017 /226
DoS Execute Code Overflow	18-09-2017	4.6	STDU Viewer 1.6.375 allows attackers to execute arbitrary code or cause a denial of service via a crafted .xps file, related to an "Illegal Instruction Violation starting at Unknown Symbol @ 0x00000000028c024d called from STDUXPSFile!DllUnregisterServer+ 0x000000000002e77b."	https://github.com/wlinzi/security_advisories/tree/master/CVE-2017-14567	A-STD-STDU - 011017 /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

			CVE ID: CVE-2017-14567		
DoS Execute Code Overflow	18-09-2017	4.6	STDU Viewer 1.6.375 allows attackers to execute arbitrary code or cause a denial of service via a crafted .xps file, related to a "User Mode Write AV starting at Unknown Symbol @ 0x00000000039d76c4 called from Unknown Symbol @ 0x0000000000049d2c." **CVE ID: CVE-2017-14566**	https://github.com/wlinzi/security_advisories/tree/master/CVE-2017-14566	A-STD-STDU - 011017 /228
DoS Overflow	18-09-2017	4.6	STDU Viewer 1.6.375 allows attackers to cause a denial of service or possibly have unspecified other impact via a crafted .xps file, related to a "Possible Stack Corruption starting at Unknown Symbol @ 0x00000000038f2fbf called from image00000000_00400000+0x0000000000240065." **CVE ID: CVE-2017-14565**	https://github.com/wlinzi/security_advisories/tree/master/CVE-2017-14565	A-STD-STDU - 011017 /229
DoS Overflow	18-09-2017	4.6	STDU Viewer 1.6.375 allows attackers to cause a denial of service or possibly have unspecified other impact via a crafted .xps file, related to "Data from Faulting Address controls Branch Selection starting at STDUXPSFile!DllUnregisterServer+0x0000000000028657." **CVE ID: CVE-2017-14564**	https://github.com/wlinzi/security_advisories/tree/master/CVE-2017-14564	A-STD-STDU - 011017 /230
DoS Execute Code Overflow	18-09-2017	4.6	STDU Viewer 1.6.375 allows attackers to execute arbitrary code or cause a denial of service via a crafted .xps file, related to a "Read Access Violation on Block Data Move starting at STDUXPSFile!DllUnregisterServer+0x0000000000005311." **CVE ID:CVE-2017-14563**	https://github.com/wlinzi/security_advisories/tree/master/CVE-2017-14563	A-STD-STDU - 011017 /231
DoS Overflow	18-09-2017	4.6	STDU Viewer 1.6.375 allows attackers to cause a denial of	https://github.com/wlinzi/se	A-STD-STDU -

			service or possibly have unspecified other impact via a crafted .xps file, related to an "Error Code (0xe06d7363) starting at wow64!Wow64NotifyDebugger+0x000000000000001d." **CVE ID: CVE-2017-14562**	curity_advisories/tree/master/CVE-2017-14562	011017/232
DoS Execute Code Overflow	18-09-2017	4.6	STDU Viewer 1.6.375 allows attackers to execute arbitrary code or cause a denial of service via a crafted .xps file, related to an "Illegal Instruction Violation starting at Unknown Symbol @ 0x00000000048c024d called from STDUXPSFile!DllUnregisterServer+0x0000000000025638." **CVE ID: CVE-2017-14561**	https://github.com/wlinzi/security_advisories/tree/master/CVE-2017-14561	A-STD-STDU - 011017/233
DoS Overflow	18-09-2017	4.6	STDU Viewer 1.6.375 allows attackers to cause a denial of service or possibly have unspecified other impact via a crafted .xps file, related to "Data from Faulting Address controls Branch Selection starting at STDUXPSFile!DllUnregisterServer+0x0000000000005bd2." **CVE ID: CVE-2017-14560**	https://github.com/wlinzi/security_advisories/tree/master/CVE-2017-14560	A-STD-STDU - 011017/234
DoS Execute Code Overflow	18-09-2017	4.6	STDU Viewer 1.6.375 allows attackers to execute arbitrary code or cause a denial of service via a crafted .xps file, related to a "Read Access Violation on Block Data Move starting at STDUXPSFile!DllUnregisterServer+0x0000000000005af2." **CVE ID: CVE-2017-14559**	https://github.com/wlinzi/security_advisories/tree/master/CVE-2017-14559	A-STD-STDU - 011017/235
DoS Execute Code Overflow	18-09-2017	4.6	STDU Viewer 1.6.375 allows attackers to execute arbitrary code or cause a denial of service via a crafted .djvu file, related to a "User Mode Write AV starting at STDUDjVuFile!DllUnregisterServer	https://github.com/wlinzi/security_advisories/tree/master/CVE-2017-14558	A-STD-STDU - 011017/236

			+0x0000000000018cc2." **CVE ID: CVE-2017-14558**		
DoS Execute Code Overflow	18-09-2017	4.6	STDU Viewer 1.6.375 allows attackers to execute arbitrary code or cause a denial of service via a crafted .djvu file, related to a "User Mode Write AV starting at STDUDjVuFile!DllUnregisterServer +0x000000000000dd3f." **CVE ID: CVE-2017-14557**	https://github.com/wlinzi/security_advisories/tree/master/CVE-2017-14557	A-STD-STDU - 011017 /237
DoS Execute Code Overflow	18-09-2017	4.6	STDU Viewer 1.6.375 allows attackers to execute arbitrary code or cause a denial of service via a crafted .djvu file, related to a "User Mode Write AV starting at STDUDjVuFile!DllUnregisterServer +0x000000000000da27." **CVE ID: CVE-2017-14556**	https://github.com/wlinzi/security_advisories/tree/master/CVE-2017-14556	A-STD-STDU - 011017 /238
DoS Overflow	18-09-2017	4.6	STDU Viewer 1.6.375 allows attackers to cause a denial of service or possibly have unspecified other impact via a crafted .djvu file, related to "Data from Faulting Address is used as one or more arguments in a subsequent Function Call starting at STDUDjVuFile!DllUnregisterServer +0x000000000000ec6e." **CVE ID: CVE-2017-14555**	https://github.com/wlinzi/security_advisories/tree/master/CVE-2017-14555	A-STD-STDU - 011017 /239
DoS Overflow	18-09-2017	4.6	STDU Viewer 1.6.375 allows attackers to cause a denial of service or possibly have unspecified other impact via a crafted .djvu file, related to a "Possible Stack Corruption starting at STDUDjVuFile!DllUnregisterServer +0x000000000000d908." **CVE ID: CVE-2017-14554**	https://github.com/wlinzi/security_advisories/tree/master/CVE-2017-14554	A-STD-STDU - 011017 /240
DoS Execute Code Overflow	18-09-2017	4.6	STDU Viewer 1.6.375 allows attackers to execute arbitrary code or cause a denial of service via a	https://github.com/wlinzi/security_advisori	A-STD-STDU - 011017

			crafted .djvu file, related to a "User Mode Write AV starting at STDUDjVuFile!DllUnregisterServer +0x00000000000085f5." **CVE ID: CVE-2017-14553**	es/tree/master/CVE-2017-14553	/241
DoS Execute Code Overflow	18-09-2017	4.6	STDU Viewer 1.6.375 allows attackers to execute arbitrary code or cause a denial of service via a crafted .djvu file, related to a "User Mode Write AV starting at STDUDjVuFile!DllUnregisterServer +0x000000000000d9a9." **CVE ID: CVE-2017-14552**	https://github.com/wlinzi/security_advisories/tree/master/CVE-2017-14552	A-STD-STDU - 011017 /242
DoS Overflow	18-09-2017	4.6	STDU Viewer 1.6.375 allows attackers to cause a denial of service or possibly have unspecified other impact via a crafted .djvu file, related to "Data from Faulting Address controls Branch Selection starting at STDUDjVuFile!DllUnregisterServer +0x000000000000d9f2." **CVE ID: CVE-2017-14551**	https://github.com/wlinzi/security_advisories/tree/master/CVE-2017-14551	A-STD-STDU - 011017 /243
DoS Overflow	18-09-2017	4.6	STDU Viewer 1.6.375 allows attackers to cause a denial of service or possibly have unspecified other impact via a crafted .djvu file, related to a "Possible Stack Corruption starting at STDUDjVuFile!DllUnregisterServer +0x000000000000e8b8." **CVE ID: CVE-2017-14550**	https://github.com/wlinzi/security_advisories/tree/master/CVE-2017-14550	A-STD-STDU - 011017 /244
DoS Execute Code Overflow	18-09-2017	4.6	STDU Viewer 1.6.375 allows attackers to execute arbitrary code or cause a denial of service via a crafted .djvu file, related to a "Heap Corruption starting at wow64!Wow64NotifyDebugger+0x000000000000001d." **CVE ID: CVE-2017-14549**	https://github.com/wlinzi/security_advisories/tree/master/CVE-2017-14549	A-STD-STDU - 011017 /245
DoS Execute Code Overflow	18-09-2017	4.6	STDU Viewer 1.6.375 allows attackers to execute arbitrary code	https://github.com/wlinzi/se	A-STD-STDU -

			or cause a denial of service via a crafted .djvu file, related to a "User Mode Write AV starting at STDUDjVuFile!DllUnregisterServer +0x000000000000854d." **CVE ID: CVE-2017-14548**	curity_advisories/tree/master/CVE-2017-14548	011017/246
DoS Overflow	18-09-2017	4.6	STDU Viewer 1.6.375 allows attackers to cause a denial of service or possibly have unspecified other impact via a crafted .mobi file, related to a "Read Access Violation starting at STDUMOBIFile!DllUnregisterServer +0x000000000002efc0." **CVE ID:CVE-2017-14547**	https://github.com/wlinzi/security_advisories/tree/master/CVE-2017-14547	A-STD-STDU - 011017/247
DoS Overflow	18-09-2017	4.6	STDU Viewer 1.6.375 allows attackers to cause a denial of service or possibly have unspecified other impact via a crafted .epub file, related to an "Error Code (0xe06d7363) starting at wow64!Wow64NotifyDebugger+0x000000000000001d." **CVE ID: CVE-2017-14546**	https://github.com/wlinzi/security_advisories/tree/master/CVE-2017-14546	A-STD-STDU - 011017/248
DoS Overflow	18-09-2017	4.6	STDU Viewer 1.6.375 allows attackers to cause a denial of service or possibly have unspecified other impact via a crafted .epub file, related to "Data from Faulting Address controls Branch Selection starting at STDUEPubFile!DllUnregisterServer +0x0000000000010332." **CVE ID: CVE-2017-14545**	https://github.com/wlinzi/security_advisories/tree/master/CVE-2017-14545	A-STD-STDU - 011017/249
DoS Overflow	18-09-2017	4.6	STDU Viewer 1.6.375 allows attackers to cause a denial of service or possibly have unspecified other impact via a crafted .epub file, related to "Data from Faulting Address is used as one or more arguments in a subsequent Function Call starting	https://github.com/wlinzi/security_advisories/tree/master/CVE-2017-14544	A-STD-STDU - 011017/250

			at STDUEPubFile!DllUnregisterServer +0x000000000003fff1." **CVE ID: CVE-2017-14544**		
DoS Overflow	18-09-2017	4.6	STDU Viewer 1.6.375 allows attackers to cause a denial of service or possibly have unspecified other impact via a crafted .epub file, related to "Data from Faulting Address controls Branch Selection starting at STDUEPubFile!DllUnregisterServer +0x0000000000039335." **CVE ID: CVE-2017-14543**	https://github.com/wlinzi/security_advisories/tree/master/CVE-2017-14543	A-STD-STDU - 011017 /251
DoS Execute Code Overflow	18-09-2017	4.6	STDU Viewer 1.6.375 allows attackers to execute arbitrary code or cause a denial of service via a crafted .epub file, related to a "Read Access Violation on Block Data Move starting at STDUEPubFile!DllUnregisterServer +0x0000000000010262." **CVE ID: CVE-2017-14542**	https://github.com/wlinzi/security_advisories/tree/master/CVE-2017-14542	A-STD-STDU - 011017 /252
DoS Execute Code Overflow	22-09-2017	4.6	STDU Viewer 1.6.375 allows attackers to execute arbitrary code or cause a denial of service via a crafted .jb2 file, related to a "User Mode Write AV starting at STDUJBIG2File!DllGetClassObject+ 0x000000000000653b." **CVE ID: CVE-2017-14692**	https://github.com/wlinzi/security_advisories/tree/master/CVE-2017-14692	A-STD-STDU - 011017 /253
DoS Overflow	22-09-2017	4.6	STDU Viewer 1.6.375 allows attackers to cause a denial of service or possibly have unspecified other impact via a crafted .jb2 file, related to "Data from Faulting Address controls Branch Selection starting at ntdll_773a0000!RtlAddAccessAllowedAce+0x000000000000027a." **CVE ID: CVE-2017-14691**	https://github.com/wlinzi/security_advisories/tree/master/CVE-2017-14691	A-STD-STDU - 011017 /254
DoS Execute Code Overflow	22-09-2017	4.6	STDU Viewer 1.6.375 allows attackers to execute arbitrary code	https://github.com/wlinzi/se	A-STD-STDU -

			or cause a denial of service via a crafted .jb2 file, related to "Data from Faulting Address controls subsequent Write Address starting at STDUJBIG2File!DllGetClassObject+0x00000000000064e7." **CVE ID: CVE-2017-14690**	curity_advisories/tree/master/CVE-2017-14690	011017/255
DoS Overflow	22-09-2017	4.6	STDU Viewer 1.6.375 allows attackers to cause a denial of service or possibly have unspecified other impact via a crafted .djvu file, related to "Data from Faulting Address is used as one or more arguments in a subsequent Function Call starting at STDUDjVuFile!DllUnregisterServer+0x000000000000328e." **CVE ID: CVE-2017-14689**	https://github.com/wlinzi/security_advisories/tree/master/CVE-2017-14689	A-STD-STDU - 011017/256
DoS Overflow	22-09-2017	4.6	STDU Viewer 1.6.375 allows attackers to cause a denial of service or possibly have unspecified other impact via a crafted .djvu file, related to a "Read Access Violation starting at STDUDjVuFile!DllUnregisterServer+0x000000000000d917." **CVE ID: CVE-2017-14688**	https://github.com/wlinzi/security_advisories/tree/master/CVE-2017-14688	A-STD-STDU - 011017/257
Sugarcrm					
Sugarcrm					
XSS	17-09-2017	4.3	An issue was discovered in SugarCRM before 7.7.2.3, 7.8.x before 7.8.2.2, and 7.9.x before 7.9.2.0 (and Sugar Community Edition 6.5.26). The WebToLeadCapture functionality is found vulnerable to unauthenticated cross-site scripting (XSS) attacks. This attack vector is mitigated by proper validating the redirect URL values being passed along.	NA	A-SUG-SUGAR-011017/258

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-2017-14510		
File Inclusion	17-09-2017	6.5	An issue was discovered in SugarCRM before 7.7.2.3, 7.8.x before 7.8.2.2, and 7.9.x before 7.9.2.0 (and Sugar Community Edition 6.5.26). A remote file inclusion has been identified in the Connectors module allowing authenticated users to include remotely accessible system files via a module=CallRest&url= query string. Proper input validation has been added to mitigate this issue. **CVE ID: CVE-2017-14509**	NA	A-SUG-SUGAR-011017/259
Sql	17-09-2017	6.5	An issue was discovered in SugarCRM before 7.7.2.3, 7.8.x before 7.8.2.2, and 7.9.x before 7.9.2.0 (and Sugar Community Edition 6.5.26). Several areas have been identified in the Documents and Emails module that could allow an authenticated user to perform SQL injection, as demonstrated by a backslash character at the end of a bean_id to modules/Emails/DetailView.php. An attacker could exploit these vulnerabilities by sending a crafted SQL request to the affected areas. An exploit could allow the attacker to modify the SQL database. Proper SQL escaping has been added to prevent such exploits. **CVE ID: CVE-2017-14508**	NA	A-SUG-SUGAR-011017/260
Suse					
Portus					
XSS	20-09-2017	3.5	Portus 2.2.0 has XSS via the Team field, related to typeahead. **CVE ID: CVE-2017-14621**	https://github.com/SUSE/Portus/pull/1425	A-SUS-PORTU-011017/261
Tapatalk					
Tapatalk					

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

Sql	21-09-2017	7.5	SQL Injection vulnerability in mobiquo/lib/classTTForum.php in the Tapatalk plugin before 4.5.8 for MyBB allows an unauthenticated remote attacker to inject arbitrary SQL commands via an XML-RPC encoded document sent as part of the user registration process. **CVE ID: CVE-2017-14652**	NA	A-TAP-TAPAT-011017/262
Tecnovision					
Dlx Spot Player4					
Execute Code	21-09-2017	6.5	Arbitrary File Upload in resource.php of TecnoVISION DLX Spot Player4 version >1.5.10 allows remote authenticated users to upload arbitrary files leading to Remote Command Execution. **CVE ID:CVE-2017-12929**	http://packetstormsecurity.com/files/144258/DlxSpot-Shell-Upload.html	A-TEC-DLX S-011017/263
Sql	21-09-2017	7.5	SQL Injection in the admin interface in TecnoVISION DLX Spot Player4 version >1.5.10 allows remote unauthenticated users to access the web interface as administrator via a crafted password. **CVE ID: CVE-2017-12930**	http://packetstormsecurity.com/files/144257/DlxSpot-SQL-Injection.html	A-TEC-DLX S-011017/264
NA	21-09-2017	10	A hard-coded password of tecn0visi0n for the dlxuser account in TecnoVISION DLX Spot Player4 (all known versions) allows remote attackers to log in via SSH and escalate privileges to root access with the same credentials. **CVE ID: CVE-2017-12928**	http://packetstormsecurity.com/files/144259/DlxSpot-Hardcoded-Password.html	A-TEC-DLX S-011017/265
Telaxius					
Epesi					
XSS	22-09-2017	3.5	In EPESI 1.8.2 rev20170830, there is Stored XSS in the Tasks Description parameter. **CVE ID: CVE-2017-14717**	https://forum.epesibim.com/d/4956-security-issue-multiple-stored-xss-in-	A-TEL-EPESI-011017/266

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

				epesi-version-1-8-2-rev20170830	
XSS	22-09-2017	3.5	In EPESI 1.8.2 rev20170830, there is Stored XSS in the Tasks Title parameter. **CVE ID: CVE-2017-14716**	https://forum.epesibim.com/d/4956-security-issue-multiple-stored-xss-in-epesi-version-1-8-2-rev20170830	A-TEL-EPESI-011017/267
XSS	22-09-2017	3.5	In EPESI 1.8.2 rev20170830, there is Stored XSS in the Tasks Alerts Title parameter. **CVE ID: CVE-2017-14715**	https://forum.epesibim.com/d/4956-security-issue-multiple-stored-xss-in-epesi-version-1-8-2-rev20170830	A-TEL-EPESI-011017/268
XSS	22-09-2017	3.5	In EPESI 1.8.2 rev20170830, there is Stored XSS in the Phonecalls Subject parameter. **CVE ID: CVE-2017-14714**	https://forum.epesibim.com/d/4956-security-issue-multiple-stored-xss-in-epesi-version-1-8-2-rev20170830	A-TEL-EPESI-011017/269
XSS	22-09-2017	3.5	In EPESI 1.8.2 rev20170830, there is Stored XSS in the Phonecalls Description parameter. **CVE ID: CVE-2017-14713**	https://forum.epesibim.com/d/4956-security-issue-multiple-stored-xss-in-epesi-version-1-8-2-rev20170830	A-TEL-EPESI-011017/270
XSS	22-09-2017	3.5	In EPESI 1.8.2 rev20170830, there is Stored XSS in the Tasks Phonecall Notes Title parameter. **CVE ID:CVE-2017-14712**	https://forum.epesibim.com/d/4956-security-issue-	A-TEL-EPESI-011017/271

				multiple-stored-xss-in-epesi-version-1-8-2-rev20170830	
Testlink					
Testlink					
Execute Code Sql	2017-09-26	7.5	SQL injection vulnerability in TestLink before 1.9.14 allows remote attackers to execute arbitrary SQL commands via the apikey parameter to lnl.php. **CVE ID: CVE-2015-7390**	http://www.securityfocus.com/archive/1/archive/1/536623/100/0/threaded	A-TES-TESTL-011017/272
Theforeman					
Foreman					
XSS	25-09-2017	4.3	Cross-site scripting (XSS) vulnerability in Foreman 1.7.0 and after. **CVE ID: CVE-2015-5282**	http://projects.theforeman.org/issues/11859	A-THE-FOREM-011017/273
Torproject					
TOR					
Gain Information	18-09-2017	4.3	The rend_service_intro_established function in or/rendservice.c in Tor before 0.2.8.15, 0.2.9.x before 0.2.9.12, 0.3.0.x before 0.3.0.11, 0.3.1.x before 0.3.1.7, and 0.3.2.x before 0.3.2.1-alpha, when SafeLogging is disabled, allows attackers to obtain sensitive information by leveraging access to the log files of a hidden service, because uninitialized stack data is included in an error message about construction of an introduction point circuit. **CVE ID: CVE-2017-0380**	https://trac.torproject.org/projects/tor/ticket/23490	A-TOR-TOR-011017/274
Trendmicro					
Mobile Security					
Execute Code	22-09-2017	6.5	Proxy command injection vulnerabilities in Trend Micro Mobile Security (Enterprise) versions before 9.7 Patch 3 allow	https://success.trendmicro.com/solution/1118224	A-TRE-MOBIL-011017/275

			remote attackers to execute arbitrary code on vulnerable installations. **CVE ID: CVE-2017-14081**		
Execute Code	22-09-2017	6.5	Unrestricted file uploads in Trend Micro Mobile Security (Enterprise) versions before 9.7 Patch 3 allow remote attackers to execute arbitrary code on vulnerable installations. **CVE ID: CVE-2017-14079**	https://success.trendmicro.com/solution/1118224	A-TRE-MOBIL-011017/276
Smart Protection Server					
Execute Code	22-09-2017	6.5	Command injection vulnerability in Trend Micro Smart Protection Server (Standalone) 3.1 and 3.2 server administration UI allows attackers with authenticated access to execute arbitrary code on vulnerable installations. **CVE ID: CVE-2017-11395**	https://success.trendmicro.com/solution/1117933	A-TRE-SMART-011017/277
Mobile Security					
Bypass	22-09-2017	7.5	Authentication bypass vulnerability in Trend Micro Mobile Security (Enterprise) versions before 9.7 Patch 3 allows attackers to access a specific part of the console using a blank password. **CVE ID: CVE-2017-14080**	https://success.trendmicro.com/solution/1118224	A-TRE-MOBIL-011017/278
Web Security Virtual Appliance					
NA	22-09-2017	9	Vulnerability issues with the web service inspection of input parameters in Trend Micro Web Security Virtual Appliance 6.5 may allow potential attackers who already have administration rights to the console to implement remote code injections. **CVE ID: CVE-2017-11396**	https://success.trendmicro.com/solution/1117412	A-TRE-WEB S-011017/279
Mobile Security					
Execute Code Sql	22-09-2017	10	SQL Injection vulnerabilities in Trend Micro Mobile Security	https://success.trendmicro.c	A-TRE-MOBIL-

			(Enterprise) versions before 9.7 Patch 3 allow remote attackers to execute arbitrary code on vulnerable installations. **CVE ID: CVE-2017-14078**	om/solution/1118224	011017/280
Twitter					
Twitter					
NA	18-09-2017	4.3	The Twitter iOS client versions 6.62 and 6.62.1 fail to validate Twitter's server certificates for the /1.1/help/settings.json configuration endpoint, permitting man-in-the-middle attackers the ability to view an application-only OAuth client token and potentially enable unreleased Twitter iOS app features. **CVE ID: CVE-2016-10511**	NA	A-TWI-TWITT-011017/281
Vbulletin					
Vbulletin					
Bypass	19-09-2017	4	vBulletin 5.x through 5.1.6 allows remote authenticated users to bypass authorization checks and inject private messages into conversations via vectors related to an input validation failure. **CVE ID: CVE-2015-3419**	http://www.vbulletin.com/forum/forum/vbulletin-announcements/vbulletin-announcements_aa/4319488-security-patch-released-for-vbulletin-5-1-4-5-1-6-and-vbulletin-cloud	A-VBU-VBULL-011017/282
Weechat					
Logger					
Overflow	23-09-2017	5	logger.c in the logger plugin in WeeChat before 1.9.1 allows a crash via strftime date/time specifiers, because a buffer is not initialized. **CVE ID: CVE-2017-**	https://weechat.org/download/security/	A-WEE-LOGGE-011017/283

			14727		
Wordpress					
Wordpress					
XSS	23-09-2017	4.3	Before version 4.8.2, WordPress was vulnerable to a cross-site scripting attack via shortcodes in the TinyMCE visual editor. **CVE ID: CVE-2017-14726**	NA	A-WOR-WORDP-011017/284
XSS	23-09-2017	4.3	Before version 4.8.2, WordPress was vulnerable to cross-site scripting in oEmbed discovery. **CVE ID: CVE-2017-14724**	NA	A-WOR-WORDP-011017/285
XSS	23-09-2017	4.3	Before version 4.8.2, WordPress allowed Cross-Site scripting in the plugin editor via a crafted plugin name. **CVE ID: CVE-2017-14721**	NA	A-WOR-WORDP-011017/286
XSS	23-09-2017	4.3	Before version 4.8.2, WordPress allowed a Cross-Site scripting attack in the template list view via a crafted template name. **CVE ID: CVE-2017-14720**	NA	A-WOR-WORDP-011017/287
XSS	23-09-2017	4.3	Before version 4.8.2, WordPress was susceptible to a Cross-Site Scripting attack in the link modal via a javascript: or data: URL. **CVE ID: CVE-2017-14718**	NA	A-WOR-WORDP-011017/288
NA	23-09-2017	4.9	Before version 4.8.2, WordPress was susceptible to an open redirect attack in wp-admin/edit-tag-form.php and wp-admin/user-edit.php. **CVE ID: CVE-2017-14725**	NA	A-WOR-WORDP-011017/289
Dir. Trav.	23-09-2017	5	Before version 4.8.2, WordPress allowed a Directory Traversal attack in the Customizer component via a crafted theme filename. **CVE ID: CVE-2017-14722**	NA	A-WOR-WORDP-011017/290
Dir. Trav.	23-09-2017	5	Before version 4.8.2, WordPress was vulnerable to a directory	NA	A-WOR-WORDP

			traversal attack during unzip operations in the ZipArchive and PclZip components. **CVE ID: CVE-2017-14719**		-011017/291
Sql	23-09-2017	7.5	Before version 4.8.2, WordPress mishandled % characters and additional placeholder values in $wpdb->prepare, and thus did not properly address the possibility of plugins and themes enabling SQL injection attacks. **CVE ID: CVE-2017-14723**	NA	A-WOR-WORDP-011017/292
Wpdevart					
Responsive Image Gallery Gallery Album					
Execute Code Sql	25-09-2017	7.5	SQL injection vulnerability in the Responsive Image Gallery plugin before 1.2.1 for WordPress allows remote attackers to execute arbitrary SQL commands via the "id" parameter in an add_edit_theme task in the wpdevart_gallery_themes page to wp-admin/admin.php. **CVE ID: CVE-2017-14125**	NA	A-WPD-RESPO-011017/293
Wpfastestcache					
Wp Fastest Cache					
CSRF	19-09-2017	6.8	Multiple cross-site request forgery (CSRF) vulnerabilities in the optionsPageRequest function in admin.php in WP Fastest Cache plugin before 0.8.3.5 for WordPress allow remote attackers to hijack the authentication of unspecified victims for requests that call the (1) saveOption, (2) deleteCache, (3) deleteCssAndJsCache, or (4) addCacheTimeout method via the wpFastestCachePage parameter in the WpFastestCacheOptions/ page. **CVE ID: CVE-2015-4089**	https://wordpress.org/plugins/wp-fastest-cache/#developers	A-WPF-WP FA-011017/294
Wso2					
Api Manager;App Manager;Application Server;Business Process Server;Business Rules					

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

Server;Complex Event Processor;Dashboard Server;Data Analytics Server;Data Services Server;Enterprise Integrator;Enterprise Mobility Manager;Governance Registry;Identity Server;Iot Server;Machine Learner;Message Broker;Storage Server					
XSS	21-09-2017	3.5	WSO2 Data Analytics Server 3.1.0 has XSS in carbon/resources/add_collection_ajaxprocessor.jsp via the collectionName or parentPath parameter. **CVE ID: CVE-2017-14651**	NA	A-WSO-API M-011017/295
Xceedium					
Xsuite					
NA	25-09-2017	5.8	Open redirect vulnerability in Xsuite 2.3.0 and 2.4.3.0 allows remote attackers to redirect users to arbitrary web sites and conduct phishing attacks via a URL in the redirurl parameter. **CVE ID: CVE-2015-4668**	NA	A-XCE-XSUIT-011017/296
Sql	25-09-2017	7.2	The MySQL "root" user in Xsuite 2.3.0 and 2.4.3.0 does not have a password set, which allows local users to access databases on the system. **CVE ID: CVE-2015-4669**	NA	A-XCE-XSUIT-011017/297
NA	25-09-2017	7.5	Multiple hardcoded credentials in Xsuite 2.3.0 and 2.4.3.0. **CVE ID: CVE-2015-4667**	NA	A-XCE-XSUIT-011017/298
Xiph					
Libvorbis					
NA	21-09-2017	4.3	In Xiph.Org libvorbis 1.3.5, an out-of-bounds array read vulnerability exists in the function mapping0_forward() in mapping0.c, which may lead to DoS when operating on a crafted audio file with vorbis_analysis(). **CVE ID: CVE-2017-14633**	https://gitlab.xiph.org/xiph/vorbis/issues/2329	A-XIP-LIBVO-011017/299
DoS Overflow	21-09-2017	6.8	The bark_noise_hybridmp function in psy.c in Xiph.Org libvorbis 1.3.5 allows remote attackers to cause a denial of service (out-of-bounds	NA	A-XIP-LIBVO-011017/300

			access and application crash) or possibly have unspecified other impact via a crafted mp4 file. **CVE ID: CVE-2017-14160**		
Execute Code Overflow	21-09-2017	7.5	Xiph.Org libvorbis 1.3.5 allows Remote Code Execution upon freeing uninitialized memory in the function vorbis_analysis_headerout() in info.c when vi->channels<=0, a similar issue to Mozilla bug 550184. **CVE ID: CVE-2017-14632**	https://gitlab.xiph.org/xiph/vorbis/issues/2328	A-XIP-LIBVO-011017/301
Xnview					
Xnview					
DoS Execute Code Overflow	18-09-2017	4.6	XnView Classic for Windows Version 2.41 allows attackers to execute arbitrary code or cause a denial of service via a crafted .jb2 file, related to a "User Mode Write AV starting at jbig2dec+0x000000000000870f."**C CVE ID: VE-2017-14580**	https://github.com/wlinzi/security_advisories/tree/master/CVE-2017-14580	A-XNV-XNVIE-011017/302
DoS Overflow	18-09-2017	4.6	XnView Classic for Windows Version 2.40 allows attackers to cause a denial of service or possibly have unspecified other impact via a crafted .svg file, related to "Data from Faulting Address controls Branch Selection starting at CADImage+0x000000000001f23e." **CVE ID: CVE-2017-14541**	https://github.com/wlinzi/security_advisories/tree/master/CVE-2017-14541	A-XNV-XNVIE-011017/303
DoS Execute Code Overflow	18-09-2017	4.6	XnView Classic for Windows Version 2.40 allows attackers to execute arbitrary code or cause a denial of service via a crafted .jb2 file, related to "Data from Faulting Address controls subsequent Write Address starting at jbig2dec+0x0000000000008823." **CVE ID: CVE-2017-14538**	https://github.com/wlinzi/security_advisories/tree/master/CVE-2017-14538	A-XNV-XNVIE-011017/304
Yadifa					
Yadifa					

NA	20-09-2017	7.8	The DNS packet parser in YADIFA before 2.2.6 does not check for the presence of infinite pointer loops, and thus it is possible to force it to enter an infinite loop. This can cause high CPU usage and makes the server unresponsive. **CVE ID: CVE-2017-14339**	https://github.com/yadifa/yadifa/blob/v2.2.6/ChangeLog	A-YAD-YADIF-011017/305
Zcms Project					
Zcms					
XSS	20-09-2017	3.5	Cross-site scripting (XSS) vulnerability in ZCMS JavaServer Pages Content Management System 1.1. **CVE ID: CVE-2015-7347**	NA	A-ZCM-ZCMS-011017/306
Zkteco					
Zktime Web					
Gain Information	21-09-2017	5	ZKTeco ZKTime Web 2.0.1.12280 allows remote attackers to obtain sensitive employee metadata via a direct request for a PDF document. **CVE ID: CVE-2017-14680**	NA	A-ZKT-ZKTIM-011017/307
CSRF	2017-09-26	6	Cross-site request forgery (CSRF) vulnerability in ZKTeco ZKTime Web 2.0.1.12280 allows remote authenticated users to hijack the authentication of administrators for requests that add administrators by leveraging lack of anti-CSRF tokens. **CVE ID: CVE-2017-13129**	NA	A-ZKT-ZKTIM-011017/308
Apache/Debian					
Http Server/Debian Linux					
NA	18-09-2017	5	Apache httpd allows remote attackers to read secret data from process memory if the Limit directive can be set in a user's .htaccess file, or if httpd.conf has certain misconfigurations, aka Optionsbleed. This affects the Apache HTTP Server through 2.2.34 and 2.4.x through 2.4.27. The attacker sends an unauthenticated	NA	A-APA-HTTP -011017/309

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

			OPTIONS HTTP request when attempting to read secret data. This is a use-after-free issue and thus secret data is not always sent, and the specific data depends on many factors including configuration. Exploitation with .htaccess can be blocked with a patch to the ap_limit_section function in server/core.c. **CVE ID: CVE-2017-9798**		
Fedoraproject/Fedoraproject					
389 Directory Server/Fedora					
Bypass	19-09-2017	5	389 Directory Server before 1.3.3.10 allows attackers to bypass intended access restrictions and modify directory entries via a crafted ldapmodrdn call. **CVE ID: CVE-2015-1854**	https://bugzilla.redhat.com/show_bug.cgi?id=1209573	A-FED-389 D-011017/310
Operating System (OS)					
ARM					
Arm-trusted-firmware					
DoS Overflow Bypass	20-09-2017	5.1	The BL1 FWU SMC handling code in ARM Trusted Firmware before 1.4 might allow attackers to write arbitrary data to secure memory, bypass the bl1_plat_mem_check protection mechanism, cause a denial of service, or possibly have unspecified other impact via a crafted AArch32 image, which triggers an integer overflow. **CVE ID: CVE-2017-9607**	https://github.com/ARM-software/arm-trusted-firmware/wiki/ARM-Trusted-Firmware-Security-Advisory-TFV-4	O-ARM-ARM-T-011017/311
Canonical					
Ubuntu Linux					
Execute Code	20-09-2017	9.3	Use-after-free vulnerability in oxide::qt::URLRequestDelegatedJob in oxide-qt in Ubuntu 15.04 and 14.04 LTS might allow remote attackers to execute arbitrary code. **CVE ID: CVE-2015-1329**	http://people.canonical.com/~ubuntu-security/cve/2015/CVE-2015-1329.html	O-CAN-UBUNT-011017/312

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

Cisco					
Unified Intelligence Center					
Execute Code XSS	21-09-2017	4.3	A vulnerability in the web interface of Cisco Unified Intelligence Center could allow an unauthenticated, remote attacker to perform a Document Object Model (DOM)-based cross-site scripting attack. The vulnerability is due to insufficient input validation of some parameters passed to the web server. An attacker could exploit this vulnerability by convincing the user to access a malicious link or by intercepting the user request and injecting the malicious code. An exploit could allow the attacker to execute arbitrary code in the context of the affected site or allow the attacker to access sensitive browser-based information. Cisco Bug IDs: CSCve76848, CSCve76856. **CVE ID: CVE-2017-12254**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170920-cuic2	O-CIS-UNIFI-011017/313
Execute Code XSS	21-09-2017	4.3	A vulnerability in the web framework code of Cisco Unified Intelligence Center Software could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web interface of an affected system. The vulnerability is due to insufficient input validation of some parameters that are passed to the web server of the affected software. An attacker could exploit this vulnerability by persuading a user to click a malicious link or by intercepting a user request and injecting malicious code into the request. A successful exploit could allow the attacker to execute arbitrary script	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170920-cuic	O-CIS-UNIFI-011017/314

			code in the context of the affected site or allow the attacker to access sensitive browser-based information. Cisco Bug IDs: CSCve76835. **CVE ID: CVE-2017-12248**		
IOS					
DoS	25-09-2017	4.9	Cisco IOS before 12.2(33)SXI allows local users to cause a denial of service (device reboot). **CVE ID: CVE-2010-3049**	https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/release/notes/ol_14271/caveats_SXI_rebuilds.html	O-CIS-IOS-011017/315
Esw2 Series Advanced Switches Firmware;Small Business 300 Series Managed Switches Firmware;Small Business 350 Series Managed Switches Firmware;Small Business 350x Series Stackable Managed Switches Firmware;Small Business 500 Series Stackable Managed Switches Firmware;Small Business 550x Series Stackable Managed Switches Firmware					
DoS Overflow	21-09-2017	5	A vulnerability in the Secure Shell (SSH) subsystem of Cisco Small Business Managed Switches software could allow an authenticated, remote attacker to cause a reload of the affected switch, resulting in a denial of service (DoS) condition. The vulnerability is due to improper processing of SSH connections. An attacker could exploit this vulnerability by logging in to an affected switch via SSH and sending a malicious SSH message. This vulnerability affects the following Cisco products when SSH is enabled: Small Business 300 Series Managed Switches, Small Business 500 Series Stackable Managed Switches, 350 Series Managed Switches, 350X Series Stackable Managed Switches, 550X	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170920-sbms	O-CIS-ESW2 - 011017/316

			Series Stackable Managed Switches, ESW2 Series Advanced Switches. Cisco Bug IDs: CSCvb48377. **CVE ID: CVE-2017-6720**		
Unified Intelligence Center					
CSRF	21-09-2017	6.8	A vulnerability in the Cisco Unified Intelligence Center could allow an unauthenticated, remote attacker to execute unwanted actions. The vulnerability is due to a lack of cross-site request forgery (CSRF) protection. An attacker could exploit this vulnerability by tricking the user of a web application into executing an adverse action. Cisco Bug IDs: CSCve76872. **CVE ID: CVE-2017-12253**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170920-cuic1	O-CIS-UNIFI-011017/317
IOS					
DoS	25-09-2017	6.8	Cisco IOS before 12.2(33)SXI allows remote authenticated users to cause a denial of service (device reboot). **CVE ID: CVE-2010-3050**	https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/release/notes/ol_14271/caveats_SXI_rebuilds.html	O-CIS-IOS-011017/318
Spa 301 Firmware;Spa 303 Firmware;Spa 500ds Firmware;Spa 500s Firmware;Spa 501g Firmware;Spa 502g Firmware;Spa 504g Firmware;Spa 508g Firmware;Spa 509g Firmware;Spa 512g Firmware;Spa 514g Firmware					
DoS	21-09-2017	7.8	A vulnerability in the handling of IP fragments for the Cisco Small Business SPA300, SPA500, and SPA51x Series IP Phones could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. The vulnerability is due to the inability to handle many large IP	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170920-spa	O-CIS-SPA 3-011017/319

			fragments for reassembly in a short duration. An attacker could exploit this vulnerability by sending a crafted stream of IP fragments to the targeted device. An exploit could allow the attacker to cause a DoS condition when the device unexpectedly reloads. Cisco Bug IDs: CSCve82586. **CVE ID: CVE-2017-12219**		
Asyncos					
DoS	21-09-2017	7.8	A vulnerability in the email message filtering feature of Cisco AsyncOS Software for the Cisco Email Security Appliance could allow an unauthenticated, remote attacker to cause an affected device to run out of memory and stop scanning and forwarding email messages. When system memory is depleted, it can cause the filtering process to crash, resulting in a denial of service (DoS) condition on the device. This vulnerability affects software version 9.0 through the first fixed release of Cisco AsyncOS Software for Cisco Email Security Appliances, both virtual and hardware appliances, if the software is configured to apply a message filter or content filter to incoming email attachments. The vulnerability is not limited to any specific rules or actions for a message filter or content filter. Cisco Bug IDs: CSCvd29354. **CVE ID: CVE-2017-12215**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170920-esa	O-CIS-ASYNC-011017/320
Google					
Android					
NA	21-09-2017	2.6	In all Qualcomm products with Android releases from CAF using the Linux kernel, potential use after	https://source.android.com/security/bullet	O-GOO-ANDRO-011017

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

			free scenarios and race conditions can occur when accessing global static variables without using a lock. **CVE ID:CVE-2017-9676**	in/2017-09-01	/321
NA	21-09-2017	2.6	In all Qualcomm products with Android releases from CAF using the Linux kernel, a race condition can allow access to already freed memory while querying event status via DCI. **CVE ID: CVE-2017-8281**	https://source.android.com/security/bulletin/2017-09-01	O-GOO-ANDRO-011017/322
Gain Information	21-09-2017	4.3	In all Qualcomm products with Android releases from CAF using the Linux kernel, when reading from sysfs nodes, one can read more information than it is allowed to. **CVE ID: CVE-2017-11040**	https://source.android.com/security/bulletin/2017-09-01	O-GOO-ANDRO-011017/323
Gain Information	21-09-2017	4.3	In all Qualcomm products with Android releases from CAF using the Linux kernel, while processing a vendor sub-command, a buffer over-read can occur.**CVE-2017-11002**	https://source.android.com/security/bulletin/2017-09-01	O-GOO-ANDRO-011017/324
Gain Information	21-09-2017	4.3	In all Qualcomm products with Android releases from CAF using the Linux kernel, the length of the MAC address is not checked which may cause out of bounds read. **CVE ID: CVE-2017-11001**	https://source.android.com/security/bulletin/2017-09-01	O-GOO-ANDRO-011017/325
Overflow	21-09-2017	5.1	In all Qualcomm products with Android releases from CAF using the Linux kernel, during the wlan calibration data store and retrieve operation, there are some potential race conditions which lead to a memory leak and a buffer overflow during the context switch. **CVE ID: CVE-2017-8280**	https://source.android.com/security/bulletin/2017-09-01	O-GOO-ANDRO-011017/326
NA	21-09-2017	6.8	In all Qualcomm products with Android releases from CAF using the Linux kernel, in an ISP Camera kernel driver function, an incorrect bounds check may potentially lead	https://source.android.com/security/bulletin/2017-09-01	O-GOO-ANDRO-011017/327

			to an out-of-bounds write. **CVE ID: CVE-2017-11000**		
Mem. Corr.	21-09-2017	6.8	In all Qualcomm products with Android releases from CAF using the Linux kernel, concurrent calls into ioctl RMNET_IOCTL_ADD_MUX_CHANNEL in ipa wan driver may lead to memory corruption due to missing locks. **CVE ID: CVE-2017-10999**	https://source.android.com/security/bulletin/2017-09-01	O-GOO-ANDRO-011017/328
Overflow	21-09-2017	6.8	In all Qualcomm products with Android releases from CAF using the Linux kernel, in audio_aio_ion_lookup_vaddr, the buffer length, which is user input, ends up being used to validate if the buffer is fully within the valid region. If the buffer length is large enough then the address + length operation could overflow and produce a result far below the valid region. **CVE ID:CVE-2017-10998**	https://source.android.com/security/bulletin/2017-09-01	O-GOO-ANDRO-011017/329
Mem. Corr.	21-09-2017	6.8	In all Qualcomm products with Android releases from CAF using the Linux kernel, using a debugfs node, a write to a PCIe register can cause corruption of kernel memory. **CVE ID:CVE-2017-10997**	https://source.android.com/security/bulletin/2017-09-01	O-GOO-ANDRO-011017/330
NA	21-09-2017	6.8	In all Qualcomm products with Android releases from CAF using the Linux kernel, due to an off-by-one error in a camera driver, an out-of-bounds read/write can occur. **CVE ID: CVE-2017-9720**	https://source.android.com/security/bulletin/2017-09-01	O-GOO-ANDRO-011017/331
Overflow	21-09-2017	6.8	In all Qualcomm products with Android releases from CAF using the Linux kernel, in function msm_compr_ioctl_shared, variable "ddp->params_length" could be accessed and modified by multiple threads, while it is not protected with locks. If one thread is running, while another thread is setting	https://source.android.com/security/bulletin/2017-09-01	O-GOO-ANDRO-011017/332

			data, race conditions will happen. If "ddp->params_length" is set to a big number, a buffer overflow will occur. **CVE ID:CVE-2017-9677**		
NA	21-09-2017	6.8	In all Qualcomm products with Android releases from CAF using the Linux kernel, in the function msm_dba_register_client, if the client registers failed, it would be freed. However the client was not removed from list. Use-after-free would occur when traversing the list next time. **CVE ID:CVE-2017-8277**	https://source.android.com/security/bulletin/2017-09-01	O-GOO-ANDRO-011017/333
Overflow	21-09-2017	6.8	In all Qualcomm products with Android releases from CAF using the Linux kernel, in functions msm_isp_check_stream_cfg_cmd & msm_isp_stats_update_cgc_override, 'stream_cfg_cmd->num_streams' is not checked, and could overflow the array stream_cfg_cmd->stream_handle. **CVE ID: CVE-2017-8251**	https://source.android.com/security/bulletin/2017-09-01	O-GOO-ANDRO-011017/334
Overflow	21-09-2017	6.8	In all Qualcomm products with Android releases from CAF using the Linux kernel, user controlled variables "nr_cmds" and "nr_bos" number are passed across functions without any check. An integer overflow to buffer overflow (with a smaller buffer allocated) may occur when they are too large or negative. **CVE ID: CVE-2017-8250**	https://source.android.com/security/bulletin/2017-09-01	O-GOO-ANDRO-011017/335
NA	21-09-2017	6.8	In all Qualcomm products with Android releases from CAF using the Linux kernel, if there is more than one thread doing the device open operation, the device may be opened more than once. This would lead to get_pid being called more than once, however put_pid	https://source.android.com/security/bulletin/2017-09-01	O-GOO-ANDRO-011017/336

			being called only once in function "msm_close".**CVE ID:CVE-2017-8247**		
Gain Information	21-09-2017	7.1	In all Qualcomm products with Android releases from CAF using the Linux kernel, out of bounds access is possible in c_show(), due to compat_hwcap_str[] not being NULL-terminated. This error is not fatal, however the device might crash/reboot with memory violation/out of bounds access. **CVE ID: CVE-2017-10996**	https://source.android.com/security/bulletin/2017-09-01	O-GOO-ANDRO-011017/337
Execute Code	25-09-2017	7.6	drivers/net/ethernet/msm/rndis_ipa.c in the Qualcomm networking driver in Android allows remote attackers to execute arbitrary code via a crafted application compromising a privileged process. **CVE ID:CVE-2016-5868**	https://source.codeaurora.org/quic/la//kernel/msm-4.4/commit/?id=fbb765a3f813f5cc85ddab21487fd65f24bf6a8c	O-GOO-ANDRO-011017/338
NA	21-09-2017	9.3	In all Qualcomm products with Android releases from CAF using the Linux kernel, an output buffer is accessed in one thread and can be potentially freed in another. **CVE ID: CVE-2017-11041**	https://source.android.com/security/bulletin/2017-09-01	O-GOO-ANDRO-011017/339
NA	21-09-2017	9.3	In all Qualcomm products with Android releases from CAF using the Linux kernel, during DMA allocation, due to wrong data type of size, allocation size gets truncated which makes allocation succeed when it should fail. **CVE ID: CVE-2017-9725**	https://source.android.com/security/bulletin/2017-09-01	O-GOO-ANDRO-011017/340
NA	21-09-2017	9.3	In all Qualcomm products with Android releases from CAF using the Linux kernel, user-level permissions can be used to gain access to kernel memory, specifically the ION cache maintenance code is writing to a	https://source.android.com/security/bulletin/2017-09-01	O-GOO-ANDRO-011017/341

			user supplied address. **CVE ID: CVE-2017-9724**		
Overflow	21-09-2017	9.3	In all Qualcomm products with Android releases from CAF using the Linux kernel, while reading audio data from an unspecified driver, a buffer overflow or integer overflow could occur. **CVE ID: CVE-2017-8278**	https://source.android.com/security/bulletin/2017-09-01	O-GOO-ANDRO-011017/342
Huawei					
P8 Firmware					
Gain Information	20-09-2017	4.3	Huawei P8 before GRA-CL00C92B210, before GRA-L09C432B200, before GRA-TL00C01B210, and before GRA-UL00C00B210 allows remote attackers to obtain user equipment (aka UE) measurements of signal strengths. **CVE ID: CVE-2015-8224**	http://www1.huawei.com/en/security/psirt/security-bulletins/security-advisories/hw-459832.htm	O-HUA-P8 FI-011017/343
Iball					
Wra150n Firmware					
Bypass	17-09-2017	10	An authentication bypass vulnerability on iBall Baton ADSL2+ Home Router FW_iB-LR7011A_1.0.2 devices potentially allows attackers to directly access administrative router settings by crafting URLs with a .cgi extension, as demonstrated by /info.cgi and /password.cgi. **CVE ID: CVE-2017-14244**	NA	O-IBA-WRA15-011017/344
Linux					
Linux Kernel					
DoS	2017-09-26	2.1	The KVM subsystem in the Linux kernel through 4.13.3 allows guest OS users to cause a denial of service (assertion failure, and hypervisor hang or crash) via an out-of bounds guest_irq value, related to arch/x86/kvm/vmx.c and virt/kvm/eventfd.c. **CVE ID: CVE-2017-1000252**	http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=36ae3c0a36b7456432fedce38ae2f7bd3e01a563	O-LIN-LINUX-011017/345

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	2017-09-26	3.6	The prepare_vmcs02 function in arch/x86/kvm/vmx.c in the Linux kernel through 4.13.3 does not ensure that the "CR8-load exiting" and "CR8-store exiting" L0 vmcs02 controls exist in cases where L1 omits the "use TPR shadow" vmcs12 control, which allows KVM L2 guest OS users to obtain read and write access to the hardware CR8 register. **CVE ID: CVE-2017-12154**	https://www.spinics.net/lists/kvm/msg155414.html	O-LIN-LINUX-011017/346
DoS	20-09-2017	4.9	The access_pmu_evcntr function in arch/arm64/kvm/sys_regs.c in the Linux kernel before 4.8.11 allows privileged KVM guest OS users to cause a denial of service (assertion failure and host OS crash) by accessing the Performance Monitors Cycle Count Register (PMCCNTR). **CVE ID: CVE-2017-12168**	https://github.com/torvalds/linux/commit/9e3f7a29694049edd728e2400ab57ad7553e5aa9	O-LIN-LINUX-011017/347
NA	21-09-2017	6.8	A security flaw was discovered in the nl80211_set_rekey_data() function in net/wireless/nl80211.c in the Linux kernel through 4.13.3. This function does not check whether the required attributes are present in a Netlink request. This request can be issued by a user with the CAP_NET_ADMIN capability and may result in a NULL pointer dereference and system crash. **CVE ID: CVE-2017-12153**	http://seclists.org/oss-sec/2017/q3/437	O-LIN-LINUX-011017/348
Qnap					
QTS					
Execute Code	19-09-2017	10	In the medialibrary component in QNAP NAS 4.3.3.0229, an un-authenticated, remote attacker can execute arbitrary system commands as the root user of the NAS application.**CVE-2017-10700**	https://www.qnap.com/en/support/con_show.php?cid=128	O-QNA-QTS-011017/349

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

Rockwellautomation					
1763-l16awa Firmware;1763-l16bbb Firmware;1763-l16bwa Firmware;1763-l16dwd Firmware					
NA	20-09-2017	5	An Improper Input Validation issue was discovered in Rockwell Automation MicroLogix 1100 controllers 1763-L16BWA, 1763-L16AWA, 1763-L16BBB, and 1763-L16DWD. A remote, unauthenticated attacker could send a single, specially crafted Programmable Controller Communication Commands (PCCC) packet to the controller that could potentially cause the controller to enter a DoS condition. **CVE ID:CVE-2017-7924**	NA	O-ROC-1763--011017/350
Sophos					
Astaro Security Gateway Firmware					
Execute Code	19-09-2017	10	Astaro Security Gateway (aka ASG) 7 allows remote attackers to execute arbitrary code via a crafted request to index.plx. **CVE ID: CVE-2017-6315**	https://www.exploit-db.com/exploits/42726/	O-SOP-ASTAR-011017/351
Tenda					
W15e Firmware					
DoS Overflow	17-09-2017	5	Heap-based Buffer Overflow on Tenda W15E devices before 15.11.0.14 allows remote attackers to cause a denial of service (temporary HTTP outage and forced logout) via unspecified vectors. **CVE ID: CVE-2017-14515**	http://www.tendacn.com/en/2018.html	O-TEN-W15E -011017/352
Dir. Trav.	17-09-2017	5	Directory Traversal on Tenda W15E devices before 15.11.0.14 allows remote attackers to read unencrypted files via a crafted URL. **CVE ID:CVE-2017-14514**	http://www.tendacn.com/en/2018.html	O-TEN-W15E -011017/353
Twsz					
Wifi Repeater Firmware					
Gain Information	20-09-2017	7.8	There is LFD (local file disclosure) on BE126 WIFI repeater 1.0 devices that allows attackers to	NA	O-TWS-WIFI -011017

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

			read the entire filesystem on the device via a crafted getpage parameter. **CVE ID: CVE-2017-8770**		/354
Execute Code	20-09-2017	10	On BE126 WIFI repeater 1.0 devices, an attacker can log into telnet (which is open by default) with default credentials as root (username:"root" password:"root") and can: 1. Read the entire file system; 2. Write to the file system; or 3. Execute any code that attacker desires (malicious or not). **CVE ID: CVE-2017-8772**	http://www.digitalwhisper.co.il/files/Zines/0x56/DW86-1-RepeaterHack.pdf	O-TWS-WIFI - 011017 /355
NA	20-09-2017	10	On BE126 WIFI repeater 1.0 devices, an attacker can log into telnet (which is open by default) with default credentials as root (username:"root" password:"root"). The attacker can make a user that is connected to the repeater click on a malicious link that will log into the telnet and will infect the device with malicious code. **CVE ID: CVE-2017-8771**	http://www.digitalwhisper.co.il/files/Zines/0x56/DW86-1-RepeaterHack.pdf	O-TWS-WIFI - 011017 /356
Utstar					
Wa3002g4 Firmware					
Bypass	17-09-2017	10	An authentication bypass vulnerability on UTStar WA3002G4 ADSL Broadband Modem WA3002G4-0021.01 devices allows attackers to directly access administrative settings and obtain cleartext credentials from HTML source, as demonstrated by info.cgi, upload.cgi, backupsettings.cgi, pppoe.cgi, resetrouter.cgi, and password.cgi. **CVE ID: CVE-2017-14243**	NA	O-UTS-WA300-011017 /357
Watchguard					
Fireware					

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

XSS	20-09-2017	4.3	An FBX-5313 issue was discovered in WatchGuard Fireware before 12.0. When a failed login attempt is made to the login endpoint of the XML-RPC interface, if JavaScript code, properly encoded to be consumed by XML parsers, is embedded as value of the user element, the code will be rendered in the context of any logged in user in the Web UI visiting "Traffic Monitor" sections "Events" and "All." As a side effect, no further events will be visible in the Traffic Monitor until the device is restarted. **CVE ID: CVE-2017-14615**	NA	O-WAT-FIREW-011017/358
NA	20-09-2017	7.8	An FBX-5312 issue was discovered in WatchGuard Fireware before 12.0. If a login attempt is made in the XML-RPC interface with an XML message containing an empty member element, the wgagent crashes, logging out any user with a session opened in the UI. By continuously executing the failed login attempts, UI management of the device becomes impossible. **CVE ID: CVE-2017-14616**	NA	O-WAT-FIREW-011017/359
ZTE					
Zxr10 1800-2s Firmware					
Dir. Trav. Gain Information	19-09-2017	5	The ZXR10 1800-2S before v3.00.40 incorrectly restricts the download of the file directory range for WEB users, resulting in the ability to download any files and cause information leaks such as system configuration. **CVE ID: CVE-2017-10931**	http://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1008262	O-ZTE-ZXR10-011017/360
NA	19-09-2017	5	The ZXR10 1800-2S before v3.00.40 incorrectly restricts access to a resource from an unauthorized actor, resulting in	http://support.zte.com.cn/support/news/LoopholeInfoDe	O-ZTE-ZXR10-011017/361

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

			ordinary users being able to download configuration files to steal information like administrator accounts and passwords. **CVE ID: CVE-2017-10930**	tail.aspx?newsId=1008262	
OS;Application (OS/A)					
Debian/Nodejs;Uronode					
Debian Linux/Node.js/Uro Node					
DoS	20-09-2017	6.8	node 0.3.2 and URONode before 1.0.5r3 allows remote attackers to cause a denial of service (bandwidth consumption). **CVE ID: CVE-2015-2927**	https://bugzilla.redhat.com/show_bug.cgi?id=1209781	O-DEB-DEBIA-011017/362
Debian Linux/Sogo					
CSRF	20-09-2017	6.8	Cross-site request forgery (CSRF) vulnerability in SOGo before 3.1.0. **CVE ID: CVE-2015-5395**	https://sogo.nu/bugs/view.php?id=3246	O-DEB-DEBIA-011017/363
Fedoraproject/Pureftpd					
Fedora/Pure-ftpd					
NA	21-09-2017	7.5	Downstream version 1.0.46-1 of pure-ftpd as shipped in Fedora was vulnerable to packaging error due to which the original configuration was ignored after update and service started running with default configuration. This has security implications because of overriding security-related configuration. This issue doesn't affect upstream version of pure-ftpd. **CVE ID: CVE-2017-12170**	https://bugzilla.redhat.com/show_bug.cgi?id=1493114	O-FED-FEDOR-011017/364
Opensuse Project/Tcpdump					
Leap/Tcpdump					
DoS	27-09-2017	5	print-wb.c in tcpdump before 4.7.4 allows remote attackers to cause a denial of service (segmentation fault and process crash). **CVE ID: CVE-2015-3138**	https://github.com/the-tcpdump-group/tcpdump/commit/3ed82f4ed0095768529afc22b92	O-OPE-LEAP/-011017/365

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

				3c8f7171fff70	

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