Vulnerability Type(s)	Publish Date	CVSS	Description CVE ID	Patch	NCIIPC ID
Application (A)					
Apache					
Commons Email					
NA	2017-08-07	5	When a call-site passes a subject for an email that contains line-breaks in Apache Commons Email 1.0 through 1.4, the caller can add arbitrary SMTP headers. **CVE-2017-9801**		A-APA-COMMO-140817/1
Cacti					
Cacti					
XSS	2017-08-01	3.5	Cross-site scripting (XSS) vulnerability in aggregate_graphs.php in Cacti before 1.1.16 allows remote authenticated users to inject arbitrary web script or HTML via specially crafted HTTP Referer headers, related to the $cancel_url variable. NOTE: this vulnerability exists because of an incomplete fix (lack of the htmlspecialchars ENT_QUOTES flag) for CVE-2017-11163. **CVE-2017-12066**	https://github.com/Cacti/cacti/commit/bd0e586f6f46d814930226f1516a194e7e72293e	A-CAC-CACTI-140817/2
Exec Code	2017-08-01	7.5	spikekill.php in Cacti before 1.1.16 might allow remote attackers to execute arbitrary code via the avgnan, outlier-start, or outlier-end parameter. **CVE-2017-12065**	https://github.com/Cacti/cacti/issues/877	A-CAC-CACTI-140817/3
Cisco					
Adaptive Security Appliance					
+Info	2017-08-07	5	A vulnerability in the web interface of the Cisco Adaptive Security Appliance (ASA) 9.3(3) and 9.6(2) could allow an unauthenticated, remote attacker to determine valid usernames. The attacker could use this information to conduct additional reconnaissance attacks. The vulnerability is due to the interaction between Lightweight	https://quickview.cloudapps.cisco.com/quickview/bug/CSCvd47888	A-CIS-ADAPT-140817/4

			Directory Access Protocol (LDAP) and SSL Connection Profile when they are configured together. An attacker could exploit the vulnerability by performing a username enumeration attack to the IP address of the device. An exploit could allow the attacker to determine valid usernames. Cisco Bug IDs: CSCvd47888. **CVE-2017-6752**		
Identity Services Engine					
Bypass	2017-08-07	7.5	A vulnerability in the authentication module of Cisco Identity Services Engine (ISE) could allow an unauthenticated, remote attacker to bypass local authentication. The vulnerability is due to improper handling of authentication requests and policy assignment for externally authenticated users. An attacker could exploit this vulnerability by authenticating with a valid external user account that matches an internal username and incorrectly receiving the authorization policy of the internal account. An exploit could allow the attacker to have Super Admin privileges for the ISE Admin portal. This vulnerability does not affect endpoints authenticating to the ISE. The vulnerability affects Cisco ISE, Cisco ISE Express, and Cisco ISE Virtual Appliance running Release 1.3, 1.4, 2.0.0, 2.0.1, or 2.1.0. Release 2.2.x is not affected. Cisco Bug IDs: CSCvb10995. **CVE-2017-6747**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170802-ise	A-CIS-IDENT-140817/5
Prime Collaboration Provisioning					
CSRF	2017-08-07	6.8	A vulnerability in the Web UI Application of the Cisco Prime Collaboration Provisioning Tool through 12.2 could allow an unauthenticated, remote attacker to execute unwanted actions. The vulnerability is due to a lack of defense	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-	A-CIS-PRIME-140817/6

			against cross-site request forgery (CSRF) attacks. An attacker could exploit this vulnerability by forcing the user's browser to perform any action authorized for that user. Cisco Bug IDs: CSCvc90280. **CVE-2017-6756**	20170802-pcpt1	
Secure Access Control System					
XSS	2017-08-07	3.5	A vulnerability in the web-based management interface of the Cisco Secure Access Control System (ACS) could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the web interface of the affected system. More Information: CSCve70587. Known Affected Releases: 5.8(0.8) 5.8(1.5). **CVE-2017-6769**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170726-acs	A-CIS-SECUR-140817/7
Smart Net Total Care Collector Appliance					
Sql	2017-08-07	4	A vulnerability in the web-based management interface of the Cisco Smart Net Total Care (SNTC) Software Collector Appliance 3.11 could allow an authenticated, remote attacker to perform a read-only, blind SQL injection attack, which could allow the attacker to compromise the confidentiality of the system through SQL timing attacks. The vulnerability is due to insufficient input validation of certain user-supplied fields that are subsequently used by the affected software to build SQL queries. An attacker could exploit this vulnerability by submitting crafted URLs, which are designed to exploit the vulnerability, to the affected software. To execute an attack successfully, the attacker would need to submit a number of requests to the affected software. A successful exploit could allow the attacker to determine the presence of values in the SQL database of the affected software.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170802-sntc	A-CIS-SMART-140817/8

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 Bug IDs: CSCvf07617. **CVE-2017-6754**		
Videoscape Distribution Suite For Television					
DoS Overflow	2017-08-07	7.8	A vulnerability in the cache server within Cisco Videoscape Distribution Suite (VDS) for Television 3.2(5)ES1 could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on a targeted appliance. The vulnerability is due to excessive mapped connections exhausting the allotted resources within the system. An attacker could exploit this vulnerability by sending large amounts of inbound traffic to a device with the intention of overloading certain resources. A successful exploit could cause the device to reload, resulting in a DoS condition. Cisco Bug IDs: CSCvc39260. **CVE-2017-6745**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170802-vds	A-CIS-VIDEO-140817/9
Clamav					
Clamav					
DoS	2017-08-06	4.3	The wwunpack function in libclamav/wwunpack.c in ClamAV 0.99.2 allows remote attackers to cause a denial of service (use-after-free) via a crafted PE file with WWPack compression. **CVE-2017-6420**	NA	A-CLA-CLAMA-140817/10
DoS	2017-08-06	4.3	libclamav/message.c in ClamAV 0.99.2 allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted e-mail message. **CVE-2017-6418**	NA	A-CLA-CLAMA-140817/11
Cs-cart					
Cs-cart Multivendor;Cs-cart.					
CSRF	2017-08-02	6.8	Cross-site request forgery (CSRF) vulnerability in CS-Cart Japanese Edition v4.3.10 and earlier (excluding v2 and v3), CS-Cart Multivendor Japanese Edition v4.3.10 and earlier (excluding v2 and v3) allows remote attackers to hijack the authentication of administrators via unspecified	NA	A-CS--CS-CA-140817/12

			vectors. **CVE-2017-2138**		
Digium					
Addons Module					
XSS	2017-08-02	4.3	Multiple cross-site scripting (XSS) vulnerabilities in views/add-license-form.php in the Digium Addons module (digiumaddoninstaller) before 2.11.0.7 for FreePBX allow remote attackers to inject arbitrary web script or HTML via the (1) add_license_key, (2) add_license_first_name, (3) add_license_last_name, (4) add_license_company, (5) add_license_address1, (6) add_license_address2, (7) add_license_city, (8) add_license_state, (9) add_license_post_code, (10) add_license_country, (11) add_license_phone, or (12) add_license_email parameter in an add-license-form page to admin/config.php. **CVE-2015-2690**	http://git.freepbx.org/projects/FREEPBX/repos/digiumaddoninstaller/commits/2aad006024b74c9ff53943d3e68527a3dffac855	A-DIG-ADDON-140817/13
Etoilewebdesign					
Ultimate Product Catalog					
XSS	2017-08-02	4.3	The Etoile Ultimate Product Catalog plugin 4.2.11 for WordPress has XSS in the Add Product Manually component. **CVE-2017-12200**	https://github.com/kevins1022/cve/blob/master/wordpress-product-catalog.md	A-ETO-ULTIM-140817/14
Ultimate Product Catalog					
Sql	2017-08-02	7.5	The Etoile Ultimate Product Catalog plugin 4.2.11 for WordPress has SQL injection with these wp-admin/admin-ajax.php POST actions: catalogue_update_order list-item, video_update_order video-item, image_update_order list-item, tag_group_update_order list_item, category_products_update_order category-product-item, custom_fields_update_order field-item,	https://github.com/kevins1022/cve/blob/master/wordpress-product-catalog.md	A-ETO-ULTIM-140817/15

			categories_update_order category-item, subcategories_update_order subcategory-item, and tags_update_order tag-list-item. **CVE-2017-12199**		
Event List Project					
Event List					
XSS	2017-08-01	4.3	The Event List plugin 0.7.9 for WordPress has XSS in the slug array parameter to wp-admin/admin.php in an el_admin_categories delete_bulk action. **CVE-2017-12068**	https://github.com/kevins1022/cve/blob/master/wordpress-event-list.md	A-EVE-EVENT-140817/16
F-secure					
F-secure Online Scanner					
Exec Code	2017-08-02	6.8	Untrusted search path vulnerability in F-Secure Online Scanner allows remote attackers to execute arbitrary code and conduct DLL hijacking attacks via a Trojan horse DLL that is located in the same folder as F-SecureOnlineScanner.exe. **CVE-2015-8264**	https://www.f-secure.com/en/web/labs_global/fsc-2015-4	A-F-S-F-SEC-140817/17
Gigaccsecure					
Gigacc Office					
NA	2017-08-02	5.5	GigaCC OFFICE ver.2.3 and earlier allows remote attackers to upload arbitrary files as a user profile image, which may be exploited for unauthorized file sharing. **CVE-2016-7845**	NA	A-GIG-GIGAC-140817/18
Exec Code	2017-08-02	6	GigaCC OFFICE ver.2.3 and earlier allows remote attackers to execute arbitrary OS commands via specially crafted mail template. **CVE-2016-7844**	NA	A-GIG-GIGAC-140817/19
Gitlab					
Gitlab					
NA	2017-08-02	4	GitLab Enterprise Edition (EE) before 8.17.7, 9.0.11, 9.1.8, 9.2.8, and 9.3.8 allows an authenticated user with the ability to create a project to use the mirroring feature to potentially read	https://about.gitlab.com/2017/07/19/gitlab-9-dot-3-dot-	A-GIT-GITLA-140817/20

			repositories belonging to other users. **CVE-2017-11437**		8-released/	
GNU						
Binutils						
Exec Code	2017-08-04	6.8	The bfd_mach_o_read_symtab_strtab function in bfd/mach-o.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29 and earlier, allows remote attackers to cause an out of bounds heap write and possibly achieve code execution via a crafted mach-o file.	**CVE-2017-12459**	https://sourceware.org/bugzilla/show_bug.cgi?id=21840	A-GNU-BINUT-140817/21
NA	2017-08-04	6.8	The nlm_swap_auxiliary_headers_in function in bfd/nlmcode.h in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29 and earlier, allows remote attackers to cause an out of bounds heap read via a crafted nlm file. **CVE-2017-12458**		https://sourceware.org/bugzilla/show_bug.cgi?id=21840	A-GNU-BINUT-140817/22
NA	2017-08-04	6.8	The bfd_make_section_with_flags function in section.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29 and earlier, allows remote attackers to cause a NULL dereference via a crafted file. **CVE-2017-12457**		https://sourceware.org/bugzilla/show_bug.cgi?id=21840	A-GNU-BINUT-140817/23
NA	2017-08-04	6.8	The read_symbol_stabs_debugging_info function in rddbg.c in GNU Binutils 2.29 and earlier allows remote attackers to cause an out of bounds heap read via a crafted binary file. **CVE-2017-12456**		https://sourceware.org/bugzilla/show_bug.cgi?id=21813	A-GNU-BINUT-140817/24
NA	2017-08-04	6.8	The evax_bfd_print_emh function in vms-alpha.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29 and earlier, allows remote attackers to cause an out of bounds heap read via a crafted vms alpha file.		https://sourceware.org/bugzilla/show_bug.cgi?id=21840	A-GNU-BINUT-140817/25

			CVE-2017-12455		
NA	2017-08-04	6.8	The _bfd_vms_slurp_egsd function in bfd/vms-alpha.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29 and earlier, allows remote attackers to cause an arbitrary memory read via a crafted vms alpha file. **CVE-2017-12454**	https://sourceware.org/bugzilla/show_bug.cgi?id=21813	A-GNU-BINUT-140817/26
NA	2017-08-04	6.8	The _bfd_vms_slurp_eeom function in libbfd.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29 and earlier, allows remote attackers to cause an out of bounds heap read via a crafted vms alpha file. **CVE-2017-12453**	https://sourceware.org/bugzilla/show_bug.cgi?id=21813	A-GNU-BINUT-140817/27
NA	2017-08-04	6.8	The bfd_mach_o_i386_canonicalize_one_reloc function in bfd/mach-o-i386.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29 and earlier, allows remote attackers to cause an out of bounds heap read via a crafted mach-o file. **CVE-2017-12452**	https://sourceware.org/bugzilla/show_bug.cgi?id=21813	A-GNU-BINUT-140817/28
NA	2017-08-04	6.8	The _bfd_xcoff_read_ar_hdr function in bfd/coff-rs6000.c and bfd/coff64-rs6000.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29 and earlier, allows remote attackers to cause an out of bounds stack read via a crafted COFF image file. **CVE-2017-12451**	https://sourceware.org/bugzilla/show_bug.cgi?id=21786	A-GNU-BINUT-140817/29
Exec Code	2017-08-04	6.8	The alpha_vms_object_p function in bfd/vms-alpha.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29 and earlier, allows remote attackers to cause an out of bounds heap write and possibly achieve code execution via a crafted vms alpha file. **CVE-2017-12450**	https://sourceware.org/bugzilla/show_bug.cgi?id=21813	A-GNU-BINUT-140817/30
NA	2017-08-04	6.8	The _bfd_vms_save_sized_string	https://sour	A-GNU-

			function in vms-misc.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29 and earlier, allows remote attackers to cause an out of bounds heap read via a crafted vms file. **CVE-2017-12449**	ceware.org/bugzilla/show_bug.cgi?id=21840	BINUT-140817/31
Exec Code	2017-08-04	6.8	The bfd_cache_close function in bfd/cache.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29 and earlier, allows remote attackers to cause a heap use after free and possibly achieve code execution via a crafted nested archive file. This issue occurs because incorrect functions are called during an attempt to release memory. The issue can be addressed by better input validation in the bfd_generic_archive_p function in bfd/archive.c. **CVE-2017-12448**	https://sourceware.org/bugzilla/show_bug.cgi?id=21787	A-GNU-BINUT-140817/32
Glibc					
NA	2017-08-01	4.3	The DNS stub resolver in the GNU C Library (aka glibc or libc6) before version 2.26, when EDNS support is enabled, will solicit large UDP responses from name servers, potentially simplifying off-path DNS spoofing attacks due to IP fragmentation. **CVE-2017-12132**	NA	A-GNU-GLIBC-140817/33
Apache					
Easy Testimonials					
XSS	2017-08-01	4.3	The Easy Testimonials plugin 3.0.4 for WordPress has XSS in include/settings/display.options.php, as demonstrated by the Default Testimonials Width, View More Testimonials Link, and Testimonial Excerpt Options screens. **CVE-2017-12131**	https://github.com/kevins1022/cve/blob/master/wordpress-Easy-Testimonials.md	A-GOL-EASY - 140817/34
Graphviz					
Graphviz					

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

DoS Exec Code Overflow	2017-08-07	6.8	Stack-based buffer overflow in the "yyerror" function in Graphviz 2.34.0 allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via a crafted file. NOTE: This vulnerability exists due to an incomplete fix for CVE-2014-0978. **CVE-2014-1235**	https://bugzilla.redhat.com/show_bug.cgi?id=1050871	A-GRA-GRAPH-140817/35
IBM					
Content Navigator					
XSS	2017-08-04	3.5	IBM Content Navigator 2.0.3 and 3.0.0 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: 126233. **CVE-2017-1331**	http://www.ibm.com/support/docview.wss?uid=swg22003928	A-IBM-CONTE-140817/36
Infosphere Information Server					
Overflow	2017-08-02	4	IBM InfoSphere Information Server 9.1, 11.3, and 11.5 could allow a privileged user to cause a memory dump that could contain highly sensitive information including access credentials. IBM X-Force ID: 128693. **CVE-2017-1495**	http://www.ibm.com/support/docview.wss?uid=swg22006068	A-IBM-INFOS-140817/37
+Priv	2017-08-02	4.6	IBM InfoSphere Information Server 9.1, 11.3, and 11.5 could allow a local user to gain elevated privileges by placing arbitrary files in installation directories. IBM X-force ID: 128467. **CVE-2017-1468**	http://www.ibm.com/support/docview.wss?uid=swg22006067	A-IBM-INFOS-140817/38
NA	2017-08-02	6.4	IBM InfoSphere Information Server 9.1, 11.3, and 11.5 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: 127155. **CVE-2017-1383**	http://www.ibm.com/support/docview.wss?uid=swg22005803	A-IBM-INFOS-140817/39
NA	2017-08-02	6.8	A network layer security vulnerability in InfoSphere Information Server 9.1,	http://www.ibm.com/su	A-IBM-INFOS-

			11.3, and 11.5 can lead to privilege escalation or unauthorized access. IBM X-Force ID: 128466. **CVE-2017-1467**	pport/docview.wss?uid=swg22006063	140817/40
Infosphere Master Data Management Server					
XSS	2017-08-03	3.5	IBM InfoSphere Master Data Management Server 10.0, 11.0, 11.3, 11.4, 11.5, and 11.6 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: 123674. **CVE-2017-1199**	http://www.ibm.com/support/docview.wss?uid=swg22006618	A-IBM-INFOS-140817/41
Inotes					
XSS	2017-08-03	4.3	IBM iNotes 8.5 and 9.0 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: 126062. **CVE-2017-1327**	http://www.ibm.com/support/docview.wss?uid=swg22003664	A-IBM-INOTE-140817/42
Mobilefirst Platform Foundation;Worklight					
XSS	2017-08-01	4.3	A Reflected Cross Site Scripting (XSS) vulnerability exists in the authorization function exposed by RESTful Web Api of IBM Worklight Framework 6.1, 6.2, 6.3, 7.0, 7.1, and 8.0. The vulnerable parameter is "scope"; if you set as its value a "realm" not defined in authenticationConfig.xml, you get an HTTP 403 Forbidden response and the value will be reflected in the body of the HTTP response. By setting it to arbitrary JavaScript code it is possible to modify the flow of the authorization function, potentially leading to credential disclosure within a trusted session. **CVE-2017-1500**	http://www-01.ibm.com/support/docview.wss?uid=swg2C1000316	A-IBM-MOBIL-140817/43
Websphere Application Server					

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	2017-08-03	4	IBM WebSphere Application Server version 9.0.0.4 could provide weaker than expected security after using the PasswordUtil command to enable AES password encryption. IBM X-Force ID: 129579. **CVE-2017-1504**	http://www.ibm.com/support/docview.wss?uid=swg22006803	A-IBM-WEBSP-140817/44
Websphere Mq Internet Pass-thru					
NA	2017-08-02	5	IBM WebSphere MQ Internet Pass-Thru 2.0 and 2.1 could allow n attacker to cause the MQIPT to stop responding due to an incorrectly configured security policy. IBM X-Force ID: 121156. **CVE-2017-1118**	http://www.ibm.com/support/docview.wss?uid=swg22006580	A-IBM-WEBSP-140817/45
IID					
Rbb Speed Test					
+Info	2017-08-02	4.3	The RBB SPEED TEST App for Android version 2.0.3 and earlier, RBB SPEED TEST App for iOS version 2.1.0 and earlier does not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate. **CVE-2017-2278**	NA	A-IID-RBB S-140817/46
Imagemagick					
Imagemagick					
DoS Overflow	2017-08-07	4.3	In ImageMagick 7.0.6-3, a memory leak vulnerability was found in the function ReadOneJNGImage in coders/png.c, which allows attackers to cause a denial of service. **CVE-2017-12676**	https://github.com/ImageMagick/ImageMagick/issues/618	A-IMA-IMAGE-140817/47
DoS Overflow	2017-08-07	4.3	In ImageMagick 7.0.6-3, a missing check for multidimensional data was found in coders/mat.c, leading to a memory leak in the function ReadImage in MagickCore/constitute.c, which allows attackers to cause a denial of service. **CVE-2017-12675**	https://github.com/ImageMagick/ImageMagick/issues/616	A-IMA-IMAGE-140817/48
DoS Overflow	2017-08-07	4.3	In ImageMagick 7.0.6-3, a memory leak vulnerability was found in the function ReadOneMNGImage in coders/png.c, which allows attackers to cause a denial	https://github.com/ImageMagick/ImageMagick	A-IMA-IMAGE-140817/49

			of service. **CVE-2017-12673**	/issues/619	
DoS Overflow	2017-08-07	4.3	In ImageMagick 7.0.6-3, a memory leak vulnerability was found in the function ReadMATImage in coders/mat.c, which allows attackers to cause a denial of service. **CVE-2017-12672**	https://github.com/ImageMagick/ImageMagick/issues/617	A-IMA-IMAGE-140817/50
DoS	2017-08-07	4.3	In ImageMagick 7.0.6-3, a missing NULL assignment was found in coders/png.c, leading to an invalid free in the function RelinquishMagickMemory in MagickCore/memory.c, which allows attackers to cause a denial of service. **CVE-2017-12671**	https://github.com/ImageMagick/ImageMagick/issues/621	A-IMA-IMAGE-140817/
DoS	2017-08-07	4.3	In ImageMagick 7.0.6-3, missing validation was found in coders/mat.c, leading to an assertion failure in the function DestroyImage in MagickCore/image.c, which allows attackers to cause a denial of service. **CVE-2017-12670**	https://github.com/ImageMagick/ImageMagick/issues/610	A-IMA-IMAGE-140817/51
DoS Overflow	2017-08-07	4.3	The ReadPICTImage function in coders/pict.c in ImageMagick 7.0.6-3 allows attackers to cause a denial of service (memory leak) via a crafted file. **CVE-2017-12654**	https://github.com/ImageMagick/ImageMagick/issues/620	A-IMA-IMAGE-140817/
DoS Overflow	2017-08-05	4.3	In ImageMagick 7.0.6-2, a memory leak vulnerability was found in the function ReadMVGImage in coders/mvg.c, which allows attackers to cause a denial of service, related to the function ReadSVGImage in svg.c. **CVE-2017-12566**	https://github.com/ImageMagick/ImageMagick/issues/603	A-IMA-IMAGE-140817/52
DoS Overflow	2017-08-05	4.3	In ImageMagick 7.0.6-2, a memory leak vulnerability was found in the function ReadOneJNGImage in coders/png.c, which allows attackers to cause a denial of service. **CVE-2017-12565**	https://github.com/ImageMagick/ImageMagick/issues/602	A-IMA-IMAGE-140817/
DoS Overflow	2017-08-05	4.3	In ImageMagick 7.0.6-2, a memory leak vulnerability was found in the function ReadMATImage in coders/mat.c, which allows attackers to cause a denial of service.	https://github.com/ImageMagick/ImageMagick/issues/601	A-IMA-IMAGE-140817/53

			CVE-2017-12564		
DoS	2017-08-04	4.3	In ImageMagick 7.0.6-1, a missing NULL check vulnerability was found in the function ReadMATImage in coders/mat.c, which allows attackers to cause a denial of service (assertion failure) in DestroyImageInfo in image.c. **CVE-2017-12434**	https://github.com/ImageMagick/ImageMagick/issues/547	A-IMA-IMAGE-140817/54
DoS Overflow	2017-08-04	4.3	In ImageMagick 7.0.6-1, a memory leak vulnerability was found in the function ReadPESImage in coders/pes.c, which allows attackers to cause a denial of service, related to ResizeMagickMemory in memory.c. **CVE-2017-12433**	https://github.com/ImageMagick/ImageMagick/issues/548	A-IMA-IMAGE-140817/55
DoS	2017-08-04	4.3	In ImageMagick 7.0.6-1, a use-after-free vulnerability was found in the function ReadWMFImage in coders/wmf.c, which allows attackers to cause a denial of service. **CVE-2017-12431**	https://github.com/ImageMagick/ImageMagick/issues/555	A-IMA-IMAGE-140817/56
DoS Overflow	2017-08-04	4.3	The ProcessMSLScript function in coders/msl.c in ImageMagick before 6.9.9-5 and 7.x before 7.0.6-5 allows remote attackers to cause a denial of service (memory leak) via a crafted file, related to the WriteMSLImage function. **CVE-2017-12427**	https://github.com/ImageMagick/ImageMagick/commit/e793eb203e5e0f91f5037aed6585e81b1e27395b	A-IMA-IMAGE-140817/57
DoS Overflow	2017-08-04	5	In ImageMagick 7.0.6-1, a memory leak vulnerability was found in the function ReadWMFImage in coders/wmf.c, which allows attackers to cause a denial of service in CloneDrawInfo in draw.c. **CVE-2017-12428**	https://github.com/ImageMagick/ImageMagick/issues/544	A-IMA-IMAGE-140817/58
Overflow	2017-08-03	5	ImageMagick 7.0.6-5 has memory leaks in the parse8BIMW and format8BIM functions in coders/meta.c, related to the WriteImage function in MagickCore/constitute.c. **CVE-2017-12418**	https://github.com/ImageMagick/ImageMagick/issues/643	A-IMA-IMAGE-140817/59
Overflow	2017-08-07	6.8	ImageMagick 7.0.6-2 has a memory leak vulnerability in WriteCALSImage in coders/cals.c.	NA	A-IMA-IMAGE-140817/

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-2017-12669		60
Overflow	2017-08-07	6.8	ImageMagick 7.0.6-2 has a memory leak vulnerability in WritePCXImage in coders/pcx.c. **CVE-2017-12668**	NA	A-IMA-IMAGE-140817/61
Overflow	2017-08-07	6.8	ImageMagick 7.0.6-1 has a memory leak vulnerability in ReadMATImage in coders\mat.c. **CVE-2017-12667**	NA	A-IMA-IMAGE-140817/62
Overflow	2017-08-07	6.8	ImageMagick 7.0.6-2 has a memory leak vulnerability in WriteINLINEImage in coders/inline.c. **CVE-2017-12666**	NA	A-IMA-IMAGE-140817/63
Overflow	2017-08-07	6.8	ImageMagick 7.0.6-2 has a memory leak vulnerability in WritePICTImage in coders/pict.c. **CVE-2017-12665**	NA	A-IMA-IMAGE-140817/64
Overflow	2017-08-07	6.8	ImageMagick 7.0.6-2 has a memory leak vulnerability in WritePALMImage in coders/palm.c. **CVE-2017-12664**	NA	A-IMA-IMAGE-140817/65
Overflow	2017-08-07	6.8	ImageMagick 7.0.6-2 has a memory leak vulnerability in WriteMAPImage in coders/map.c. **CVE-2017-12663**	NA	A-IMA-IMAGE-140817/66
Overflow	2017-08-07	6.8	ImageMagick 7.0.6-2 has a memory leak vulnerability in WritePDFImage in coders/pdf.c. **CVE-2017-12662**	NA	A-IMA-IMAGE-140817/67
Overflow	2017-08-07	6.8	ImageMagick 7.0.6-1 has a memory leak vulnerability in ReadDCMImage in coders\dcm.c. **CVE-2017-12644**	https://github.com/ImageMagick/ImageMagick/commit/9f375e7080a2c1044cd546854d0548b4bfb429d0	A-IMA-IMAGE-140817/68
Overflow	2017-08-07	6.8	ImageMagick 7.0.6-1 has a memory leak vulnerability in ReadMPCImage in coders\mpc.c. **CVE-2017-12642**	https://github.com/ImageMagick/ImageMagick/issues/552	A-IMA-IMAGE-140817/69
Overflow	2017-08-07	6.8	ImageMagick 7.0.6-1 has a memory leak vulnerability in ReadOneJNGImage in	https://github.com/Ima	A-IMA-IMAGE-

			coders\png.c. **CVE-2017-12641**	geMagick/ImageMagick/commit/3320955045e5a2a22c13a04fa9422bb809e75eda	140817/70
NA	2017-08-07	6.8	ImageMagick 7.0.6-1 has an out-of-bounds read vulnerability in ReadOneMNGImage in coders/png.c. **CVE-2017-12640**	https://github.com/ImageMagick/ImageMagick/issues/542	A-IMA-IMAGE-140817/71
NA	2017-08-06	6.8	ImageMagick 7.0.6-1 has a large loop vulnerability in the ReadPWPImage function in coders\pwp.c. **CVE-2017-12587**	https://github.com/ImageMagick/ImageMagick/issues/535	A-IMA-IMAGE-140817/72
NA	2017-08-07	6.8	coders/wpg.c in ImageMagick allows remote attackers to have unspecified impact via a corrupted wpg file. **CVE-2014-9831**	https://bugzilla.redhat.com/show_bug.cgi?id=1343487	A-IMA-IMAGE-140817/73
NA	2017-08-07	6.8	coders/sun.c in ImageMagick allows remote attackers to have unspecified impact via a corrupted sun file. **CVE-2014-9830**	https://anonscm.debian.org/cgit/collab-maint/imagemagick.git/commit/?h=debian-patches/6.8.9.9-4-for-upstream&id=b68b78e2625122d9f6b6d88ba4df7e85b47b556f	A-IMA-IMAGE-140817/74
NA	2017-08-07	6.8	coders/psd.c in ImageMagick allows remote attackers to have unspecified impact via a crafted psd file. **CVE-2014-9828**	https://anonscm.debian.org/cgit/collab-maint/imagemagick.git/commit/?h=	A-IMA-IMAGE-140817/75

				debian-patches/6.8.9.9-4-for-upstream&id=460547be494cc8c039b99b65e64a1fa2eb08ab5c	
NA	2017-08-07	6.8	coders/xpm.c in ImageMagick allows remote attackers to have unspecified impact via a crafted xpm file. **CVE-2014-9827**	https://anonscm.debian.org/cgit/collab-maint/imagemagick.git/commit/?h=debian-patches/6.8.9.9-4-for-upstream&id=69490f5cffbda612e15a2985699455bb0b45e276	A-IMA-IMAGE-140817/76
DoS	2017-08-07	7.1	In ImageMagick 7.0.6-2, a CPU exhaustion vulnerability was found in the function ReadPDBImage in coders/pdb.c, which allows attackers to cause a denial of service. **CVE-2017-12674**	https://github.com/ImageMagick/ImageMagick/issues/604	A-IMA-IMAGE-140817/77
NA	2017-08-07	7.1	ImageMagick 7.0.6-1 has a memory exhaustion vulnerability in ReadOneJNGImage in coders\png.c. **CVE-2017-12643**	https://github.com/ImageMagick/ImageMagick/commit/9eedb5660f1704cde8e8cd784c5c2a09dd2fd60f	A-IMA-IMAGE-140817/78
DoS	2017-08-05	7.1	In ImageMagick 7.0.6-2, a memory exhaustion vulnerability was found in the function ReadPSDImage in coders/psd.c, which allows attackers to cause a denial of service.	https://github.com/ImageMagick/ImageMagick/issues/599	A-IMA-IMAGE-140817/79

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-2017-12563		
DoS	2017-08-04	7.1	In ImageMagick 7.0.6-1, a memory exhaustion vulnerability was found in the function ReadPCXImage in coders/pcx.c, which allows attackers to cause a denial of service. **CVE-2017-12432**	https://github.com/ImageMagick/ImageMagick/issues/536	A-IMA-IMAGE-140817/80
NA	2017-08-02	7.1	The ReadDCMImage function in coders\dcm.c in ImageMagick 7.0.6-1 has an integer signedness error leading to excessive memory consumption via a crafted DCM file. **CVE-2017-12140**	https://github.com/ImageMagick/ImageMagick/issues/533	A-IMA-IMAGE-140817/81
DoS	2017-08-04	7.8	In ImageMagick 7.0.6-1, a memory exhaustion vulnerability was found in the function ReadSUNImage in coders/sun.c, which allows attackers to cause a denial of service. **CVE-2017-12435**	https://github.com/ImageMagick/ImageMagick/issues/543	A-IMA-IMAGE-140817/82
DoS	2017-08-04	7.8	In ImageMagick 7.0.6-1, a memory exhaustion vulnerability was found in the function ReadMPCImage in coders/mpc.c, which allows attackers to cause a denial of service. **CVE-2017-12430**	https://github.com/ImageMagick/ImageMagick/issues/546	A-IMA-IMAGE-140817/83
DoS	2017-08-04	7.8	In ImageMagick 7.0.6-1, a memory exhaustion vulnerability was found in the function ReadMIFFImage in coders/miff.c, which allows attackers to cause a denial of service. **CVE-2017-12429**	https://github.com/ImageMagick/ImageMagick/issues/545	A-IMA-IMAGE-140817/84
Ioquake3					
Ioquake3					
DoS Overflow	2017-08-03	7.5	Buffer overflow in ioquake3 before 2017-08-02 allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted packet. **CVE-2017-11721**	https://github.com/ioquake/ioq3/commit/d2b1d124d4055c2fcbe5126863487c52fd58cca1	A-IOQ-IOQUA-140817/85
Joomla					
Joomla!					
NA	2017-08-02	6.5	The CMS installer in Joomla! before 3.7.4 does not verify a user's ownership	https://developer.jooml	A-JOO-JOOML-

			of a webspace, which allows remote authenticated users to gain control of the target application by leveraging Certificate Transparency logs. **CVE-2017-11364**	a.org/security-centre/700-20170704-core-installer-lack-of-ownership-verification.html	140817/86
Kiri					
Tween					
+Priv	2017-08-02	9.3	Untrusted search path vulnerability in Tween Ver1.6.6.0 and earlier allows an attacker to gain privileges via a Trojan horse DLL in an unspecified directory. **CVE-2017-2279**	https://jvn.jp/en/jp/JVN17523256/index.html	A-KIR-TWEEN-140817/87
Ledger-cli					
Ledger					
DoS Overflow	2017-08-04	6.8	The ledger::parse_date_mask_routine function in times.cc in Ledger 3.1.1 allows remote attackers to cause a denial of service (stack-based buffer overflow and application crash) or possibly have unspecified other impact via a crafted file. **CVE-2017-12482**	http://bugs.ledger-cli.org/show_bug.cgi?id=1224	A-LED-LEDGE-140817/88
DoS Overflow	2017-08-04	6.8	The find_option function in option.cc in Ledger 3.1.1 allows remote attackers to cause a denial of service (stack-based buffer overflow and application crash) or possibly have unspecified other impact via a crafted file. **CVE-2017-12481**	http://bugs.ledger-cli.org/show_bug.cgi?id=1222	A-LED-LEDGE-140817/89
Lhaforge Project					
Lhaforge					
+Priv	2017-08-02	6.8	Untrusted search path vulnerability in LhaForge Ver.1.6.5 and earlier allows an attacker to gain privileges via a Trojan horse DLL in an unspecified directory. **CVE-2017-2288**	https://jvn.jp/en/jp/JVN74554973/index.html	A-LHA-LHAFO-140817/90
Libmspack Project					
Libmspack					

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

DoS Overflow	2017-08-06	6.8	mspack/lzxd.c in libmspack 0.5alpha, as used in ClamAV 0.99.2, 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 CHM file.	**CVE-2017-6419**	NA	A-LIB-LIBMS-140817/91
Libquicktime						
Libquicktime						
DoS	2017-08-02	4.3	In libquicktime 1.2.4, an allocation failure was found in the function quicktime_read_ftyp in ftyp.c, which allows attackers to cause a denial of service via a crafted file. **CVE-2017-12145**		NA	A-LIB-LIBQU-140817/92
DoS	2017-08-02	4.3	In libquicktime 1.2.4, an allocation failure was found in the function quicktime_read_info in lqt_quicktime.c, which allows attackers to cause a denial of service via a crafted file. **CVE-2017-12143**		NA	A-LIB-LIBQU-140817/93
Libsndfile Project						
Libsndfile						
DoS Overflow	2017-08-05	7.5	Heap-based Buffer Overflow in the psf_binheader_writef function in common.c in libsndfile through 1.0.28 allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact.	**CVE-2017-12562**	https://github.com/erikd/libsndfile/issues/292	A-LIB-LIBSN-140817/94
Liferay						
Liferay Portal						
XSS	2017-08-07	4.3	XSS exists in Liferay Portal before 7.0 CE GA4 via a crafted title or summary that is mishandled in the Web Content Display. **CVE-2017-12649**		https://dev.liferay.com/web/community-security-team/known-vulnerabilities/liferay-	A-LIF-LIFER-140817/95

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

				portal-70/-/asset_publisher/cjE0ourZXJZE/content/cst-7017-multiple-xss-vulnerabilities	
XSS	2017-08-07	4.3	XSS exists in Liferay Portal before 7.0 CE GA4 via a bookmark URL. **CVE-2017-12648**	https://dev.liferay.com/web/community-security-team/known-vulnerabilities/liferay-portal-70/-/asset_publisher/cjE0ourZXJZE/content/cst-7017-multiple-xss-vulnerabilities	A-LIF-LIFER-140817/96
XSS	2017-08-07	4.3	XSS exists in Liferay Portal before 7.0 CE GA4 via a Knowledge Base article title. **CVE-2017-12647**	https://dev.liferay.com/web/community-security-team/known-vulnerabilities/liferay-portal-70/-/asset_publisher/cjE0ourZXJZE/content/cst-7017-multiple-	A-LIF-LIFER-140817/97

				xss-vulnerabilities	
XSS	2017-08-07	4.3	XSS exists in Liferay Portal before 7.0 CE GA4 via a login name, password, or e-mail address. **CVE-2017-12646**	https://dev.liferay.com/web/community-security-team/known-vulnerabilities/liferay-portal-70/-/asset_publisher/cjE0ourZXJZE/content/cst-7017-multiple-xss-vulnerabilities	A-LIF-LIFER-140817/98
XSS	2017-08-07	4.3	XSS exists in Liferay Portal before 7.0 CE GA4 via an invalid portletId. **CVE-2017-12645**	https://dev.liferay.com/web/community-security-team/known-vulnerabilities/liferay-portal-70/-/asset_publisher/cjE0ourZXJZE/content/cst-7017-multiple-xss-vulnerabilities	A-LIF-LIFER-140817/99
XSS	2017-08-07	4.3	XSS exists in Liferay Portal before 7.0 CE GA4 via a crafted redirect field to modules/apps/foundation/frontend-js/frontend-js-spa-	https://dev.liferay.com/web/community-	A-LIF-LIFER-140817/100

			web/src/main/resources/META-INF/resources/init.jsp. **CVE-2016-10404**	security-team/known-vulnerabilities/liferay-portal-70/-/asset_publisher/cjE0ourZXJZE/content/cst-7017-multiple-xss-vulnerabilities	
Mantisbt					
Mantisbt					
+Info	2017-08-01	3.5	The "Project Documentation" feature in MantisBT 1.2.19 and earlier, when the threshold to access files ($g_view_proj_doc_threshold) is set to ANYBODY, allows remote authenticated users to download attachments linked to arbitrary private projects via a file id number in the file_id parameter to file_download.php. **CVE-2015-5059**	https://github.com/mantisbt/mantisbt/commit/f39cf5251953b468e9d921e1cf2aca3abdb00772	A-MAN-MANTI-140817/101
+Info	2017-08-05	4	If, after successful installation of MantisBT through 2.5.2 on MySQL/MariaDB, the administrator does not remove the 'admin' directory (as recommended in the "Post-installation and upgrade tasks" section of the MantisBT Admin Guide), and the MySQL client has a local_infile setting enabled (in php.ini mysqli.allow_local_infile, or the MySQL client config file, depending on the PHP setup), an attacker may take advantage of MySQL's "connect file read" feature to remotely access files on the MantisBT server. **CVE-2017-12419**	https://mantisbt.org/bugs/view.php?id=23173	A-MAN-MANTI-140817/102
Microsoft					
Outlook;Outlook 2013 Rt					

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

+Info	2017-08-01	4.3	Microsoft Outlook 2007 SP3, Outlook 2010 SP2, Outlook 2013 SP1, Outlook 2013 RT SP1, and Outlook 2016 as packaged in Microsoft Office allows an information disclosure vulnerability due to the way that it discloses the contents of its memory, aka "Microsoft Office Outlook Information Disclosure Vulnerability". **CVE-2017-8572**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8572	A-MIC-OUTLO-140817/103
Bypass	2017-08-01	6.8	Microsoft Outlook 2007 SP3, Outlook 2010 SP2, Outlook 2013 SP1, Outlook 2013 RT SP1, and Outlook 2016 as packaged in Microsoft Office allows a security feature bypass vulnerability due to the way that it handles input, aka "Microsoft Office Outlook Security Feature Bypass Vulnerability". **CVE-2017-8571**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8571	A-MIC-OUTLO-140817/104
Exec Code Mem. Corr.	2017-08-01	9.3	Microsoft Outlook 2007 SP3, Outlook 2010 SP2, Outlook 2013 SP1, Outlook 2013 RT SP1, and Outlook 2016 as packaged in Microsoft Office allows a remote code execution vulnerability due to the way Microsoft Outlook parses specially crafted email messages, aka "Microsoft Office Outlook Memory Corruption Vulnerability" **CVE-2017-8663**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8663	A-MIC-OUTLO-140817/105
Mufg					
Mitsubishi Ufj					
NA	2017-08-02	4.3	The Bank of Tokyo-Mitsubishi UFJ, Ltd. App for Android ver5.3.1, ver5.2.2 and earlier allow a man-in-the-middle attacker to downgrade the communication between the app and the server from TLS v1.2 to SSL v3.0, which may result in the attacker to eavesdrop on an encrypted communication. **CVE-2016-7812**	NA	A-MUF-MITSU-140817/106
Netapp					
Snapcenter Server					
NA	2017-08-07	6.5	NetApp SnapCenter Server 1.0 allows remote authenticated users to list and	https://kb.netapp.com/s	A-NET-SNAPC-

			delete backups. **CVE-2015-7887**	upport/s/article/ka51A00000007EnQAI/authentication-bypass-vulnerability-in-snapcenter-server-1-0?language=en_US	140817/107
Nitro					
Nitro Pro					
Exec Code Dir. Trav.	2017-08-03	6.8	Nitro Pro 11.0.3.173 allows remote attackers to execute arbitrary code via saveAs and launchURL calls with directory traversal sequences. **CVE-2017-7442**	NA	A-NIT-NITRO-140817/108
Opencv					
Opencv					
NA	2017-08-06	6.8	OpenCV (Open Source Computer Vision Library) through 3.3 has an out-of-bounds write error in the function FillColorRow4 in utils.cpp when reading an image file by using cv::imread. **CVE-2017-12606**	NA	A-OPE-OPENC-140817/109
NA	2017-08-06	6.8	OpenCV (Open Source Computer Vision Library) through 3.3 has an out-of-bounds write error in the FillColorRow8 function in utils.cpp when reading an image file by using cv::imread. **CVE-2017-12605**	NA	A-OPE-OPENC-140817/110
NA	2017-08-06	6.8	OpenCV (Open Source Computer Vision Library) through 3.3 has an out-of-bounds write error in the FillUniColor function in utils.cpp when reading an image file by using cv::imread. **CVE-2017-12604**	NA	A-OPE-OPENC-140817/111
Overflow	2017-08-06	6.8	OpenCV (Open Source Computer Vision Library) through 3.3 has an invalid write in the cv::RLByteStream::getBytes function in	NA	A-OPE-OPENC-140817/112

			modules/imgcodecs/src/bitstrm.cpp when reading an image file by using cv::imread, as demonstrated by the 2-opencv-heapoverflow-fseek test case. **CVE-2017-12603**		
Overflow	2017-08-06	6.8	OpenCV (Open Source Computer Vision Library) through 3.3 has a buffer overflow in the cv::BmpDecoder::readData function in modules/imgcodecs/src/grfmt_bmp.cpp when reading an image file by using cv::imread, as demonstrated by the 4-buf-overflow-readData-memcpy test case. **CVE-2017-12601**	NA	A-OPE-OPENC-140817/113
NA	2017-08-06	6.8	OpenCV (Open Source Computer Vision Library) through 3.3 has an out-of-bounds read error in the function icvCvt_BGRA2BGR_8u_C4C3R when reading an image file by using cv::imread. **CVE-2017-12599**	NA	A-OPE-OPENC-140817/114
NA	2017-08-06	6.8	OpenCV (Open Source Computer Vision Library) through 3.3 has an out-of-bounds read error in the cv::RBaseStream::readBlock function in modules/imgcodecs/src/bitstrm.cpp when reading an image file by using cv::imread, as demonstrated by the 8-opencv-invalid-read-fread test case. **CVE-2017-12598**	NA	A-OPE-OPENC-140817/115
NA	2017-08-06	6.8	OpenCV (Open Source Computer Vision Library) through 3.3 has an out-of-bounds write error in the function FillColorRow1 in utils.cpp when reading an image file by using cv::imread. **CVE-2017-12597**	NA	A-OPE-OPENC-140817/116
DoS	2017-08-06	7.8	OpenCV (Open Source Computer Vision Library) through 3.3 has a denial of service (memory consumption) issue, as demonstrated by the 10-opencv-dos-memory-exhaust test case. **CVE-2017-12602**	NA	A-OPE-OPENC-140817/117
DoS	2017-08-06	7.8	OpenCV (Open Source Computer Vision	NA	A-OPE-

			Library) through 3.3 has a denial of service (CPU consumption) issue, as demonstrated by the 11-opencv-dos-cpu-exhaust test case. **CVE-2017-12600**		OPENC-140817/118
Open-emr					
Openemr					
Bypass	2017-08-01	5	The csv_log_html function in library/edihistory/edih_csv_inc.php in OpenEMR 5.0.0 and prior allows attackers to bypass intended access restrictions via a crafted name. **CVE-2017-12064**	https://github.com/openemr/openemr/commit/b8963a5ca483211ed8de71f18227a0e66a2582ad	A-OPE-OPENE-140817/119
Oracle					
Agile Product Lifecycle Management Framework					
NA	2017-08-08	3.6	Vulnerability in the Oracle Agile PLM component of Oracle Supply Chain Products Suite (subcomponent: Security). Supported versions that are affected are 9.3.5 and 9.3.6. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle Agile PLM executes to compromise Oracle Agile PLM. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Agile PLM accessible data as well as unauthorized read access to a subset of Oracle Agile PLM accessible data. CVSS 3.0 Base Score 3.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:N). **CVE-2017-10088**	http://www.oracle.com/technetwork/security-advisory/cpujul2017-3236622.html	A-ORA-AGILE-140817/120
+Info	2017-08-08	5	Vulnerability in the Oracle Agile PLM component of Oracle Supply Chain Products Suite (subcomponent: Security). Supported versions that are affected are 9.3.5 and 9.3.6. Easily exploitable vulnerability allows	http://www.oracle.com/technetwork/security-advisory/cpujul2017-	A-ORA-AGILE-140817/121

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

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

			unauthenticated attacker with network access via HTTP to compromise Oracle Agile PLM. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Agile PLM accessible data. CVSS 3.0 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE-2017-10093**	3236622.html	
NA	2017-08-08	5.8	Vulnerability in the Oracle Agile PLM component of Oracle Supply Chain Products Suite (subcomponent: Security). Supported versions that are affected are 9.3.5 and 9.3.6. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Agile PLM. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Agile PLM, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Agile PLM accessible data as well as unauthorized read access to a subset of Oracle Agile PLM accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE-2017-10092**	http://www.oracle.com/technetwork/security-advisory/cpujul2017-3236622.html	A-ORA-AGILE-140817/122
NA	2017-08-08	5.8	Vulnerability in the Oracle Agile PLM component of Oracle Supply Chain Products Suite (subcomponent: Security). Supported versions that are affected are 9.3.5 and 9.3.6. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Agile PLM. Successful attacks require	http://www.oracle.com/technetwork/security-advisory/cpujul2017-3236622.html	A-ORA-AGILE-140817/123

			human interaction from a person other than the attacker and while the vulnerability is in Oracle Agile PLM, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Agile PLM accessible data as well as unauthorized read access to a subset of Oracle Agile PLM accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE-2017-10082**		
NA	2017-08-08	5.8	Vulnerability in the Oracle Agile PLM component of Oracle Supply Chain Products Suite (subcomponent: PCMServlet). Supported versions that are affected are 9.3.5 and 9.3.6. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Agile PLM. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Agile PLM, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Agile PLM accessible data as well as unauthorized read access to a subset of Oracle Agile PLM accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE-2017-10052**	http://www.oracle.com/technetwork/security-advisory/cpujul2017-3236622.html	A-ORA-AGILE-140817/124
Business Intelligence Publisher					
NA	2017-08-08	4.9	Vulnerability in the BI Publisher component of Oracle Fusion Middleware (subcomponent: Mobile	http://www.oracle.com/technetwor	A-ORA-BUSIN-140817/

			Service). The supported version that is affected is 11.1.1.7.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise BI Publisher. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in BI Publisher, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all BI Publisher accessible data as well as unauthorized update, insert or delete access to some of BI Publisher accessible data. CVSS 3.0 Base Score 7.6 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:L/A:N). **CVE-2017-10059**	k/security-advisory/cpujul2017-3236622.html	125
NA	2017-08-08	4.9	Vulnerability in the BI Publisher component of Oracle Fusion Middleware (subcomponent: Web Server). Supported versions that are affected are 11.1.1.9.0, 12.2.1.1.0 and 12.2.1.2.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise BI Publisher. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in BI Publisher, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all BI Publisher accessible data as well as unauthorized update, insert or delete access to some of BI Publisher accessible data. CVSS 3.0 Base Score 7.6 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:L/A:N). **CVE-2017-10041**	http://www.oracle.com/technetwork/security-advisory/cpujul2017-3236622.html	A-ORA-BUSIN-140817/126

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

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

NA	2017-08-08	5.8	Vulnerability in the BI Publisher component of Oracle Fusion Middleware (subcomponent: BI Publisher Security). Supported versions that are affected are 11.1.1.7.0 and 11.1.1.9.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise BI Publisher. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in BI Publisher, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all BI Publisher accessible data as well as unauthorized update, insert or delete access to some of BI Publisher accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N). **CVE-2017-10043**	http://www.oracle.com/technetwork/security-advisory/cpujul2017-3236622.html	A-ORA-BUSIN-140817/127
NA	2017-08-08	5.8	Vulnerability in the BI Publisher component of Oracle Fusion Middleware (subcomponent: Web Server). Supported versions that are affected are 11.1.1.7.0 and 11.1.1.9.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise BI Publisher. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in BI Publisher, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all BI Publisher accessible data as well as unauthorized update, insert or delete access to some of BI Publisher accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity	http://www.oracle.com/technetwork/security-advisory/cpujul2017-3236622.html	A-ORA-BUSIN-140817/128

			impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N). **CVE-2017-10035**		
NA	2017-08-08	5.8	Vulnerability in the BI Publisher component of Oracle Fusion Middleware (subcomponent: Web Server). The supported version that is affected is 11.1.1.7.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise BI Publisher. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in BI Publisher, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all BI Publisher accessible data as well as unauthorized update, insert or delete access to some of BI Publisher accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N). **CVE-2017-10030**	http://www.oracle.com/technetwork/security-advisory/cpujul2017-3236622.html	A-ORA-BUSIN-140817/129
NA	2017-08-08	5.8	Vulnerability in the BI Publisher component of Oracle Fusion Middleware (subcomponent: Web Server). The supported version that is affected is 11.1.1.7.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise BI Publisher. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in BI Publisher, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all BI Publisher accessible data as well as unauthorized	http://www.oracle.com/technetwork/security-advisory/cpujul2017-3236622.html	A-ORA-BUSIN-140817/130

			update, insert or delete access to some of BI Publisher accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N). **CVE-2017-10029**		
NA	2017-08-08	5.8	Vulnerability in the BI Publisher component of Oracle Fusion Middleware (subcomponent: Web Server). The supported version that is affected is 11.1.1.7.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise BI Publisher. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in BI Publisher, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all BI Publisher accessible data as well as unauthorized update, insert or delete access to some of BI Publisher accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N). **CVE-2017-10028**	http://www.oracle.com/technetwork/security-advisory/cpujul2017-3236622.html	A-ORA-BUSIN-140817/131
NA	2017-08-08	5.8	Vulnerability in the BI Publisher component of Oracle Fusion Middleware (subcomponent: Layout Tools). The supported version that is affected is 11.1.1.7.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise BI Publisher. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in BI Publisher, attacks may significantly impact additional products. Successful attacks of this vulnerability can result	http://www.oracle.com/technetwork/security-advisory/cpujul2017-3236622.html	A-ORA-BUSIN-140817/132

			in unauthorized access to critical data or complete access to all BI Publisher accessible data as well as unauthorized update, insert or delete access to some of BI Publisher accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N). **CVE-2017-10024**		
NA	2017-08-08	6.4	Vulnerability in the BI Publisher component of Oracle Fusion Middleware (subcomponent: BI Publisher Security). The supported version that is affected is 11.1.1.7.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise BI Publisher. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all BI Publisher accessible data as well as unauthorized update, insert or delete access to some of BI Publisher accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N). **CVE-2017-10025**	http://www.oracle.com/technetwork/security-advisory/cpujul2017-3236622.html	A-ORA-BUSIN-140817/133
Enterprise Manager Base Platform					
NA	2017-08-08	4	Vulnerability in the Enterprise Manager Base Platform component of Oracle Enterprise Manager Grid Control (subcomponent: UI Framework). Supported versions that are affected are 12.1.0, 13.1.0 and 13.2.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Enterprise Manager Base Platform. While the vulnerability is in Enterprise Manager Base Platform, attacks may significantly impact additional products. Successful attacks of this vulnerability can result	http://www.oracle.com/technetwork/security-advisory/cpujul2017-3236622.html	A-ORA-ENTER-140817/134

			in unauthorized creation, deletion or modification access to critical data or all Enterprise Manager Base Platform accessible data. CVSS 3.0 Base Score 7.7 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:N/I:H/A:N). **CVE-2017-10091**		
Flexcube Private Banking					
NA	2017-08-08	4	Vulnerability in the Oracle FLEXCUBE Private Banking component of Oracle Financial Services Applications (subcomponent: Miscellaneous). Supported versions that are affected are 2.0.0, 2.0.1, 2.2.0 and 12.0.1. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle FLEXCUBE Private Banking. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle FLEXCUBE Private Banking accessible data. CVSS 3.0 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N). **CVE-2017-10007**	http://www.oracle.com/technetwork/security-advisory/cpujul2017-3236622.html	A-ORA-FLEXC-140817/135
NA	2017-08-08	4	Vulnerability in the Oracle FLEXCUBE Private Banking component of Oracle Financial Services Applications (subcomponent: Miscellaneous). Supported versions that are affected are 2.0.0, 2.0.1, 2.2.0 and 12.0.1. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle FLEXCUBE Private Banking. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle FLEXCUBE Private Banking accessible data. CVSS 3.0 Base Score 6.5 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:N).	http://www.oracle.com/technetwork/security-advisory/cpujul2017-3236622.html	A-ORA-FLEXC-140817/136

			CVE-2017-10006		
NA	2017-08-08	5.8	Vulnerability in the Oracle FLEXCUBE Private Banking component of Oracle Financial Services Applications (subcomponent: Miscellaneous). Supported versions that are affected are 2.0.0, 2.0.1, 2.2.0 and 12.0.1. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle FLEXCUBE Private Banking. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle FLEXCUBE Private Banking, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle FLEXCUBE Private Banking accessible data as well as unauthorized read access to a subset of Oracle FLEXCUBE Private Banking accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE-2017-10005**	http://www.oracle.com/technetwork/security-advisory/cpujul2017-3236622.html	A-ORA-FLEXC-140817/137
Hospitality Inventory Management					
NA	2017-08-08	5.5	Vulnerability in the Oracle Hospitality Inventory Management component of Oracle Hospitality Applications (subcomponent: Settings and Config). Supported versions that are affected are 8.5.1 and 9.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hospitality Inventory Management. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Hospitality Inventory Management accessible data as well as unauthorized read access to a	http://www.oracle.com/technetwork/security-advisory/cpujul2017-3236622.html	A-ORA-HOSPI-140817/138

			subset of Oracle Hospitality Inventory Management accessible data. CVSS 3.0 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N). **CVE-2017-10002**		
Hospitality Reporting And Analytics					
NA	2017-08-08	4	Vulnerability in the Oracle Hospitality Reporting and Analytics component of Oracle Hospitality Applications (subcomponent: Reporting). Supported versions that are affected are 8.5.1 and 9.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hospitality Reporting and Analytics. While the vulnerability is in Oracle Hospitality Reporting and Analytics, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Hospitality Reporting and Analytics. CVSS 3.0 Base Score 7.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H). **CVE-2017-10000**	http://www.oracle.com/technetwork/security-advisory/cpujul2017-3236622.html	A-ORA-HOSPI-140817/139
Hospitality Simphony					
NA	2017-08-08	6	Vulnerability in the Oracle Hospitality Simphony First Edition component of Oracle Hospitality Applications (subcomponent: Core). The supported version that is affected is 1.7.1. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hospitality Simphony First Edition. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized	http://www.oracle.com/technetwork/security-advisory/cpujul2017-3236622.html	A-ORA-HOSPI-140817/140

			access to critical data or complete access to all Oracle Hospitality Simphony First Edition accessible data as well as unauthorized update, insert or delete access to some of Oracle Hospitality Simphony First Edition accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Hospitality Simphony First Edition. CVSS 3.0 Base Score 7.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:L/A:H). **CVE-2017-10001**		
Hospitality Websuite8 Cloud Service					
NA	2017-08-08	5.8	Vulnerability in the Hospitality WebSuite8 Cloud Service component of Oracle Hospitality Applications (subcomponent: General). Supported versions that are affected are 8.9.6 and 8.10.x. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Hospitality WebSuite8 Cloud Service. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Hospitality WebSuite8 Cloud Service, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Hospitality WebSuite8 Cloud Service accessible data as well as unauthorized read access to a subset of Hospitality WebSuite8 Cloud Service accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE-2017-10064**	http://www.oracle.com/technetwork/security-advisory/cpujul2017-3236622.html	A-ORA-HOSPI-140817/141

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

Micros Bellavita					
NA	2017-08-08	6.4	Vulnerability in the MICROS BellaVita component of Oracle Hospitality Applications (subcomponent: Interface). The supported version that is affected is 2.7.x. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise MICROS BellaVita. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MICROS BellaVita accessible data as well as unauthorized read access to a subset of MICROS BellaVita accessible data. CVSS 3.0 Base Score 6.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N). **CVE-2017-10047**	http://www.oracle.com/technetwork/security-advisory/cpujul2017-3236622.html	A-ORA-MICRO-140817/142
Pcfreetime					
Format Factory					
NA	2017-08-03	7.5	Format Factory 4.1.0 has a DLL Hijacking Vulnerability because an untrusted search path is used for msimg32.dll, WindowsCodecs.dll, and dwmapi.dll. **CVE-2017-12414**	http://www.kth.ninja/2017/08/format-factory-dll-hijacking.html	A-PCF-FORMA-140817/143
Pega					
Pega Platform					
+Info	2017-08-02	4	The application distribution export functionality in PEGA Platform 7.2 ML0 and earlier allows remote authenticated users with certain privileges to obtain sensitive configuration information by leveraging a missing access control. **CVE-2017-11356**	NA	A-PEG-PEGA -140817/144
XSS	2017-08-02	4.3	Multiple cross-site scripting (XSS) vulnerabilities in PEGA Platform 7.2 ML0 and earlier allow remote attackers to inject arbitrary web script or HTML via the (1) PATH_INFO to the main page; the (2) beanReference parameter	NA	A-PEG-PEGA -140817/145

			to the JavaBean viewer page; or the (3) pyTableName to the System database schema modification page. **CVE-2017-11355**		
Potrace Project					
Potrace					
NA	2017-08-01	5	Potrace 1.14 has a heap-based buffer over-read in the interpolate_cubic function in mkbitmap.c. **CVE-2017-12067**	https://github.com/hackerlib/hackerlib-vul/tree/master/potrace/heap-buffer-overflow-mkbitmap	A-POT-POTRA-140817/146
Qemu					
Qemu					
DoS	2017-08-02	2.1	The address_space_write_continue function in exec.c in QEMU (aka Quick Emulator) allows local guest OS privileged users to cause a denial of service (out-of-bounds access and guest instance crash) by leveraging use of qemu_map_ram_ptr to access guest ram block area. **CVE-2017-11334**	https://bugzilla.redhat.com/show_bug.cgi?id=1471638	A-QEM-QEMU-140817-147
DoS Overflow	2017-08-02	2.1	Stack-based buffer overflow in hw/usb/redirect.c in QEMU (aka Quick Emulator) allows local guest OS users to cause a denial of service (QEMU process crash) via vectors related to logging debug messages. **CVE-2017-10806**	https://bugzilla.redhat.com/show_bug.cgi?id=1468496	A-QEM-QEMU-140817-148
DoS	2017-08-02	5	qemu-nbd in QEMU (aka Quick Emulator) does not ignore SIGPIPE, which allows remote attackers to cause a denial of service (daemon crash) by disconnecting during a server-to-client reply attempt. **CVE-2017-10664**	NA	A-QEM-QEMU-140817/149
Razerzone					
Razer Synapse					
NA	2017-08-02	2.1	A specially crafted IOCTL can be issued	https://war	A-RAZ-

			to the rzpnk.sys driver in Razer Synapse that can cause an out of bounds read operation to occur due to a field within the IOCTL data being used as a length. **CVE-2017-9770**		room.secure state.com/cve-2017-9770/	RAZER 140817/150
NA	2017-08-02	10	A specially crafted IOCTL can be issued to the rzpnk.sys driver in Razer Synapse 2.20.15.1104 that is forwarded to ZwOpenProcess allowing a handle to be opened to an arbitrary process. **CVE-2017-9769**		NA	A-RAZ-RAZER-140817/151
Simple Custom Css And Js						
XSS	2017-08-02	4.3	Cross-site scripting vulnerability in Simple Custom CSS and JS prior to version 3.4 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	**CVE-2017-2285**	NA	A-SIL-SIMPL-140817/152
Stashcat						
Heinekingmedia						
NA	2017-08-01	4	An issue was discovered in heinekingmedia StashCat through 1.7.5 for Android, through 0.0.80w for Web, and through 0.0.86 for Desktop. It uses RSA to exchange a secret for symmetric encryption of messages. However, the private RSA key is not only stored on the client but transmitted to the backend, too. Moreover, the key to decrypt the private key is composed of the first 32 bytes of the SHA-512 hash of the user password. But this hash is stored on the backend, too. Therefore, everyone with access to the backend database can read the transmitted secret for symmetric encryption, hence can read the communication. **CVE-2017-11136**		http://seclists.org/fulldisclosure/2017/Jul/90	A-STA-HEINE-140817/153
NA	2017-08-01	4	An issue was discovered in heinekingmedia StashCat through 1.7.5 for Android. The login credentials are written into a log file on the device. Hence, an attacker with access to the logs can read them.		http://seclists.org/fulldisclosure/2017/Jul/90	A-STA-HEINE-140817/154

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

			CVE-2017-11134		
NA	2017-08-01	4.3	An issue was discovered in heinekingmedia StashCat through 1.7.5 for Android, through 0.0.80w for Web, and through 0.0.86 for Desktop. For authentication, the user password is hashed directly with SHA-512 without a salt or another key-derivation mechanism to enable a secure secret for authentication. Moreover, only the first 32 bytes of the hash are used. This allows for easy dictionary and rainbow-table attacks if an attacker has access to the password hash. **CVE-2017-11131**	http://seclists.org/fulldisclosure/2017/Jul/90	A-STA-HEINE-140817/155
DoS	2017-08-01	5	An issue was discovered in heinekingmedia StashCat through 1.7.5 for Android, through 0.0.80w for Web, and through 0.0.86 for Desktop. The logout mechanism does not check for authorization. Therefore, an attacker only needs to know the device ID. This causes a denial of service. This might be interpreted as a vulnerability in customer-controlled software, in the sense that the StashCat client side has no secure way to signal that it is ending a session and that data should be deleted. **CVE-2017-11135**	http://seclists.org/fulldisclosure/2017/Jul/90	A-STA-HEINE-140817/156
NA	2017-08-01	5	An issue was discovered in heinekingmedia StashCat through 1.7.5 for Android, through 0.0.80w for Web, and through 0.0.86 for Desktop. To encrypt messages, AES in CBC mode is used with a pseudo-random secret. This secret and the IV are generated with math.random() in previous versions and with CryptoJS.lib.WordArray.random() in newer versions, which uses math.random() internally. This is not cryptographically strong. **CVE-2017-11133**	http://seclists.org/fulldisclosure/2017/Jul/90	A-STA-HEINE-140817/157
NA	2017-08-01	5	An issue was discovered in	http://seclis	A-STA-

			heinekingmedia StashCat before 1.5.18 for Android. No certificate pinning is implemented; therefore the attacker could issue a certificate for the backend and the application would not notice it. **CVE-2017-11132**	ts.org/fulldisclosure/2017/Jul/90	HEINE-140817/158
NA	2017-08-01	6.8	An issue was discovered in heinekingmedia StashCat through 1.7.5 for Android, through 0.0.80w for Web, and through 0.0.86 for Desktop. The product's protocol only tries to ensure confidentiality. In the whole protocol, no integrity or authenticity checks are done. Therefore man-in-the-middle attackers can conduct replay attacks. **CVE-2017-11130**	http://seclists.org/fulldisclosure/2017/Jul/90	A-STA-HEINE-140817/159
NA	2017-08-01	7.5	An issue was discovered in heinekingmedia StashCat through 1.7.5 for Android. The keystore is locked with a hard-coded password. Therefore, everyone with access to the keystore can read the content out, for example the private key of the user. **CVE-2017-11129**	http://seclists.org/fulldisclosure/2017/Jul/90	A-STA-HEINE-140817/160
Sugarcrm					
Sugarcrm					
Exec Code	2017-08-07	4.6	Incomplete blacklist vulnerability in SugarCRM 6.5.22 allows local users to execute arbitrary code by uploading a file with an executable extension. **CVE-2015-5946**	NA	A-SUG-SUGAR-140817/161
Trello					
Trello					
XSS	2017-08-02	4.3	Cross-site scripting (XSS) vulnerability in the Trello app before 4.0.8 for iOS might allow remote attackers to inject arbitrary web script or HTML by uploading and attaching a crafted photo to a Card. **CVE-2017-9244**	https://hackerone.com/reports/227853	A-TRE-TRELL-140817/162
Trendmicro					
Control Manager					
NA	2017-08-02	5	XML external entity (XXE) processing vulnerability in Trend Micro Control	NA	A-TRE-CONTR-

			Manager 6.0, if exploited, could lead to information disclosure. Formerly ZDI-CAN-4706. **CVE-2017-11390**		140817/163
Bypass +Info	2017-08-02	5	Authentication Bypass in Trend Micro Control Manager 6.0 causes Information Disclosure when authentication validation is not done for functionality that can change debug logging level. Formerly ZDI-CAN-4512. **CVE-2017-11387**	NA	A-TRE-CONTR-140817/164
Exec Code Sql	2017-08-02	6.5	SQL Injection in Trend Micro Control Manager 6.0 causes Remote Code Execution when RestfulServiceUtility.NET.dll doesn't properly validate user provided strings before constructing SQL queries. Formerly ZDI-CAN-4639 and ZDI-CAN-4638. **CVE-2017-11388**	NA	A-TRE-CONTR-140817/165
Exec Code Dir. Trav.	2017-08-02	7.5	Directory traversal vulnerability in Trend Micro Control Manager 6.0 allows remote code execution by attackers able to drop arbitrary files in a web-facing directory. Formerly ZDI-CAN-4684. **CVE-2017-11389**	NA	A-TRE-CONTR-140817/166
Exec Code Sql	2017-08-02	7.5	SQL Injection in Trend Micro Control Manager 6.0 causes Remote Code Execution when executing opcode 0x4707 due to lack of proper user input validation in cmdHandlerNewReportScheduler.dll. Formerly ZDI-CAN-4549. **CVE-2017-11386**	NA	A-TRE-CONTR-140817/167
Exec Code Sql	2017-08-02	7.5	SQL Injection in Trend Micro Control Manager 6.0 causes Remote Code Execution when executing opcode 0x6b1b due to lack of proper user input validation in cmdHandlerStatusMonitor.dll. Formerly ZDI-CAN-4545. **CVE-2017-11385**	NA	A-TRE-CONTR-140817/168
Exec Code Sql	2017-08-02	7.5	SQL Injection in Trend Micro Control Manager 6.0 causes Remote Code	NA	A-TRE-CONTR-

			Execution when executing opcode 0x3b21 due to lack of proper user input validation in mdHandlerLicenseManager.dll. Formerly ZDI-CAN-4561. **CVE-2017-11384**		140817/169
Exec Code Sql	2017-08-02	7.5	SQL Injection in Trend Micro Control Manager 6.0 causes Remote Code Execution when executing opcode 0x1b07 due to lack of proper user input validation in cmdHandlerTVCSCommander.dll. Formerly ZDI-CAN-4560. **CVE-2017-11383**	NA	A-TRE-CONTR-140817/170
Deep Discovery Director					
NA	2017-08-01	5	Configuration and database backup archives are not signed or validated in Trend Micro Deep Discovery Director 1.1. **CVE-2017-11379**	https://success.trendmicro.com/solution/1117663	A-TRE-DEEP - 140817/171
NA	2017-08-01	7.5	A command injection vulnerability exists in Trend Micro Deep Discovery Director 1.1 that allows an attacker to restore accounts that can access the pre-configuration console. **CVE-2017-11381**	https://success.trendmicro.com/solution/1117663	A-TRE-DEEP - 140817/172
NA	2017-08-01	7.5	Backup archives were found to be encrypted with a static password across different installations, which suggest the same password may be used in all virtual appliance instances of Trend Micro Deep Discovery Director 1.1. **CVE-2017-11380**	https://success.trendmicro.com/solution/1117663	A-TRE-DEEP - 140817/173
Deep Discovery Email Inspector					
DoS	2017-08-03	6.4	Denial of Service vulnerability in Trend Micro Deep Discovery Email Inspector 2.5.1 allows remote attackers to delete arbitrary files on vulnerable installations, thus disabling the service. Formerly ZDI-CAN-4350. **CVE-2017-11382**	NA	A-TRE-DEEP - 140817/174
Interscan Messaging Security Virtual Appliance					
Exec Code	2017-08-03	6.5	Proxy command injection vulnerability in Trend Micro InterScan Messaging Virtual Appliance 9.0 and 9.1 allows	NA	A-TRE-INTER-140817/

			remote attackers to execute arbitrary code on vulnerable installations. The specific flaw can be exploited by parsing the "T" parameter within modTMCSS Proxy. Formerly ZDI-CAN-4745. **CVE-2017-11392**		175
Exec Code	2017-08-03	6.5	Proxy command injection vulnerability in Trend Micro InterScan Messaging Virtual Appliance 9.0 and 9.1 allows remote attackers to execute arbitrary code on vulnerable installations. The specific flaw can be exploited by parsing the "t" parameter within modTMCSS Proxy. Formerly ZDI-CAN-4744. **CVE-2017-11391**	NA	A-TRE-INTER-140817/176
Officescan					
Exec Code	2017-08-03	10	Proxy command injection vulnerability in Trend Micro OfficeScan 11 and XG (12) allows remote attackers to execute arbitrary code on vulnerable installations. The specific flaw can be exploited by parsing the T parameter within Proxy.php. Formerly ZDI-CAN-4544. **CVE-2017-11394**	NA	A-TRE-OFFIC-140817/177
Exec Code	2017-08-03	10	Proxy command injection vulnerability in Trend Micro OfficeScan 11 and XG (12) allows remote attackers to execute arbitrary code on vulnerable installations. The specific flaw can be exploited by parsing the tr parameter within Proxy.php. Formerly ZDI-CAN-4543. **CVE-2017-11393**	NA	A-TRE-OFFIC-140817/178
Underbit					
Mad Libmad					
DoS Overflow Mem. Corr.	2017-08-01	4.3	The mad_decoder_run function in decoder.c in libmad 0.15.1b allows remote attackers to cause a denial of service (memory corruption) via a crafted MP3 file. **CVE-2017-11552**	NA	A-UND-MAD L-140817/179
Unit4					

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

Teta Web					
NA	2017-08-02	7.5	Session fixation vulnerability in Unit4 Polska TETA Web (formerly TETA Galactica) 22.62.3.4 and earlier allows remote attackers to hijack web sessions via a session id. **CVE-2015-1174**	http://packetstormsecurity.com/files/133296/UNIT4TETA-TETA-WEB-22.62.3.4-Session-Fixation.html	A-UNI-TETA - 140817/180
Unitrends					
Backup					
Exec Code	2017-08-07	9	It was discovered that an issue in the session logic in Unitrends Backup (UB) before 10.0.0 allowed using the LOGDIR environment variable during a web session to elevate an existing low-privilege user to root privileges. A remote attacker with existing low-privilege credentials could then execute arbitrary commands with root privileges. **CVE-2017-12479**	https://support.unitrends.com/UnitrendsBackup/s/article/000005757	A-UNI-BACKU-140817/181
Exec Code Bypass	2017-08-07	10	It was discovered that the api/storage web interface in Unitrends Backup (UB) before 10.0.0 has an issue in which one of its input parameters was not validated. A remote attacker could use this flaw to bypass authentication and execute arbitrary commands with root privilege on the target system. **CVE-2017-12478**	https://support.unitrends.com/UnitrendsBackup/s/article/000005756	A-UNI-BACKU-140817/182
Exec Code Bypass	2017-08-07	10	It was discovered that the bpserverd proprietary protocol in Unitrends Backup (UB) before 10.0.0, as invoked through xinetd, has an issue in which its authentication can be bypassed. A remote attacker could use this issue to execute arbitrary commands with root privilege on the target system. **CVE-2017-12477**	https://support.unitrends.com/UnitrendsBackup/s/article/000005755	A-UNI-BACKU-140817/183
Vmware					
Vcenter Server					

+Info	2017-08-01	4	VMware vCenter Server (6.5 prior to 6.5 U1) contains an information disclosure issue due to the service startup script using world writable directories as temporary storage for critical information. Successful exploitation of this issue may allow unprivileged host users to access certain critical information when the service gets restarted. **CVE-2017-4922**	https://www.vmware.com/security/advisories/VMSA-2017-0013.html	A-VMW-VCENT-140817/184
+Info	2017-08-01	5	VMware vCenter Server (6.5 prior to 6.5 U1) contains an information disclosure vulnerability. This issue may allow plaintext credentials to be obtained when using the vCenter Server Appliance file-based backup feature. **CVE-2017-4923**	https://www.vmware.com/security/advisories/VMSA-2017-0013.html	A-VMW-VCENT-140817/185
NA	2017-08-01	6.5	VMware vCenter Server (6.5 prior to 6.5 U1) contains an insecure library loading issue that occurs due to the use of LD_LIBRARY_PATH variable in an unsafe manner. Successful exploitation of this issue may allow unprivileged host users to load a shared library that may lead to privilege escalation. **CVE-2017-4921**	https://www.vmware.com/security/advisories/VMSA-2017-0013.html	A-VMW-VCENT-140817/186
Wppopupmaker					
Popup Maker					
XSS	2017-08-02	4.3	Cross-site scripting vulnerability in Popup Maker prior to version 1.6.5 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors. **CVE-2017-2284**	NA	A-WPP-POPUP-140817/187
Xoops					
Xoops					
XSS	2017-08-02	4.3	XOOPS Core 2.5.8 has stored XSS in imagemanager.php because of missing MIME type validation in htdocs/class/uploader.php. **CVE-2017-12139**	https://github.com/XOOPS/XoopsCore25/issues/524	A-XOO-XOOPS-140817/188
Bypass	2017-08-02	5.8	XOOPS Core 2.5.8 has a stored URL redirect bypass vulnerability in /modules/profile/index.php because of	https://github.com/XOOPS/XoopsC	A-XOO-XOOPS-140817/

			the URL filter. **CVE-2017-12138**	ore25/issues/523	189
Yeager					
Yeager Cms					
Exec Code	2017-08-07	6.8	Unrestricted file upload vulnerability in Yeager CMS 1.2.1 allows remote attackers to execute arbitrary code by uploading a file with an executable extension. **CVE-2015-7571**	NA	A-YEA-YEAGE-140817/190
Ytnef Project					
Ytnef					
DoS	2017-08-02	4.3	In ytnef 1.9.2, an allocation failure was found in the function TNEFFillMapi in ytnef.c, which allows attackers to cause a denial of service via a crafted file. **CVE-2017-12144**	NA	A-YTN-YTNEF-140817/191
DoS	2017-08-02	4.3	In ytnef 1.9.2, an invalid memory read vulnerability was found in the function SwapDWord in ytnef.c, which allows attackers to cause a denial of service via a crafted file. **CVE-2017-12142**	NA	A-YTN-YTNEF-140817/192
DoS Overflow	2017-08-02	4.3	In ytnef 1.9.2, a heap-based buffer overflow vulnerability was found in the function TNEFFillMapi in ytnef.c, which allows attackers to cause a denial of service via a crafted file. **CVE-2017-12141**	NA	A-YTN-YTNEF-140817/193
Hardware (H)					
Citrix					
Netscaler Application Delivery Controller;Netscaler Gateway					
+Info	2017-08-02	4.3	The TLS and DTLS processing functionality in Citrix NetScaler Application Delivery Controller (ADC) and NetScaler Gateway devices with firmware 9.x before 9.3 Build 68.5, 10.0 through Build 78.6, 10.1 before Build 130.13, 10.1.e before Build 130.1302.e, 10.5 before Build 55.8, and 10.5.e before Build 55.8007.e makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, a variant of CVE-2014-	http://support.citrix.com/article/CTX200378	H-CIT-NETSC-140817/194

			3566 (aka POODLE). **CVE-2015-3642**		
Operating System (O)					
Cisco					
IOS					
DoS	2017-08-02	6.8	Cisco IOS before 15.2(4)S6 does not initialize an unspecified variable, which might allow remote authenticated users to cause a denial of service (CPU consumption, watchdog timeout, crash) by walking specific SNMP objects. **CVE-2012-5030**	https://www.cisco.com/c/en/us/td/docs/ios/15_2s/release/notes/15_2s_rel_notes/15_2s_caveats_15_2_4s.html	O-CIS-IOS-140817/195
Ios Xe					
NA	2017-08-07	5	A vulnerability in the Autonomic Networking feature of Cisco IOS XE Software could allow an unauthenticated, remote, autonomic node to access the Autonomic Networking infrastructure of an affected system, after the certificate for the autonomic node has been revoked. This vulnerability affected devices that are running Release 16.x of Cisco IOS XE Software and are configured to use Autonomic Networking. This vulnerability does not affect devices that are running an earlier release of Cisco IOS XE Software or devices that are not configured to use Autonomic Networking. More Information: CSCvd22328. Known Affected Releases: 15.5(1)S3.1 Denali-16.2.1. **CVE-2017-6664**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170726-anicrl	O-CIS-IOS X-140817/196
IOS;Ios Xe					
+Info	2017-08-07	3.3	A vulnerability in the Autonomic Networking feature of Cisco IOS Software and Cisco IOS XE Software could allow an unauthenticated, adjacent attacker to reset the Autonomic Control Plane (ACP) of an affected system and view ACP packets that are transferred in clear text within	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170726-	O-CIS-IOS;Ios-140817/197

			an affected system, an Information Disclosure Vulnerability. More Information: CSCvd51214. Known Affected Releases: Denali-16.2.1 Denali-16.3.1. **CVE-2017-6665**	aniacp	
DoS	2017-08-07	6.1	A vulnerability in the Autonomic Networking feature of Cisco IOS Software and Cisco IOS XE Software could allow an unauthenticated, adjacent attacker to cause autonomic nodes of an affected system to reload, resulting in a denial of service (DoS) condition. More Information: CSCvd88936. Known Affected Releases: Denali-16.2.1 Denali-16.3.1. **CVE-2017-6663**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170726-anidos	O-CIS-IOS;I-140817/198
Google					
Android					
DoS	2017-08-07	2.1	The updateMessageStatus function in Android 5.1.1 and earlier allows local users to cause a denial of service (NULL pointer exception and process crash). **CVE-2015-3839**	https://huntcve.github.io/2017/02/13/cveupdate/	O-GOO-ANDRO-140817/199
Iodata					
Wn-ax1167gr Firmware					
Exec Code Overflow	2017-08-02	5.2	Buffer overflow in WN-AX1167GR firmware version 3.00 and earlier allows an attacker to execute arbitrary commands via unspecified vectors. **CVE-2017-2282**	NA	O-IOD-WN-AX-140817/200
Exec Code	2017-08-02	8.3	WN-AX1167GR firmware version 3.00 and earlier allows an attacker to execute arbitrary OS commands via unspecified vectors. **CVE-2017-2281**	NA	O-IOD-WN-AX-140817/201
Exec Code	2017-08-02	8.3	WN-AX1167GR firmware version 3.00 and earlier uses hardcoded credentials which may allow an attacker that can access the device to execute arbitrary code on the device. **CVE-2017-2280**	NA	O-IOD-WN-AX-140817/202
Wn-g300r3 Firmware					
Exec Code	2017-08-02	5.8	WN-G300R3 firmware version 1.0.2 and earlier uses hardcoded credentials	NA	O-IOD-WN-G3-

			which may allow an attacker that can access the device to execute arbitrary code on the device. **CVE-2017-2283**		140817/203
Linux					
Linux Kernel					
DoS +Priv Mem. Corr.	2017-08-05	6.9	Race condition in the fsnotify implementation in the Linux kernel through 4.12.4 allows local users to gain privileges or cause a denial of service (memory corruption) via a crafted application that leverages simultaneous execution of the inotify_handle_event and vfs_rename functions. **CVE-2017-7533**	NA	O-LIN-LINUX-140817/204
Oracle					
Solaris					
DoS	2017-08-08	4.4	Vulnerability in the Solaris component of Oracle Sun Systems Products Suite (subcomponent: Network Services Library). The supported version that is affected is 10. Difficult to exploit vulnerability allows low privileged attacker with logon to the infrastructure where Solaris executes to compromise Solaris. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Solaris accessible data as well as unauthorized read access to a subset of Solaris accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Solaris. CVSS 3.0 Base Score 4.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:L). **CVE-2017-10003**	http://www.oracle.com/technetwork/security-advisory/cpujul2017-3236622.html	O-ORA-SOLAR-140817/205
NA	2017-08-08	7.2	Vulnerability in the Solaris component of Oracle Sun Systems Products Suite (subcomponent: Kernel). Supported versions that are affected are 10 and 11. Easily exploitable vulnerability allows	http://www.oracle.com/technetwork/security-advisory/cp	O-ORA-SOLAR-140817/206

			high privileged attacker with logon to the infrastructure where Solaris executes to compromise Solaris. Successful attacks of this vulnerability can result in takeover of Solaris. CVSS 3.0 Base Score 6.7 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H). **CVE-2017-10004**	ujul2017-3236622.html	
Paloaltonetworks					
Pan-os					
XSS	2017-08-02	4.3	Cross-site scripting (XSS) vulnerability in the GlobalProtect external interface in Palo Alto Networks PAN-OS before 6.1.18, 7.x before 7.0.16, 7.1.x before 7.1.11, and 8.x before 8.0.3 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors. **CVE-2017-9467**	https://securityadvisories.paloaltonetworks.com/Home/Detail/90	O-PAL-PAN-O-140817/207
XSS	2017-08-02	4.3	Cross-site scripting (XSS) vulnerability in the management web interface in Palo Alto Networks PAN-OS before 6.1.18, 7.x before 7.0.16, 7.1.x before 7.1.11, and 8.x before 8.0.3 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors. **CVE-2017-9459**	https://securityadvisories.paloaltonetworks.com/Home/Detail/89	O-PAL-PAN-O-140817/208
Exec Code	2017-08-02	10	The DNS Proxy in Palo Alto Networks PAN-OS before 6.1.18, 7.x before 7.0.16, 7.1.x before 7.1.11, and 8.x before 8.0.3 allows remote attackers to execute arbitrary code via a crafted domain name. **CVE-2017-8390**	https://securityadvisories.paloaltonetworks.com/Home/Detail/91	O-PAL-PAN-O-140817/209
Samsung					
Samsung Mobile					
NA	2017-08-02	4.4	Race condition in the ioctl implementation in the Samsung Graphics 2D driver (aka /dev/fimg2d) in Samsung devices with Android L(5.0/5.1) allows local users to trigger memory errors by leveraging definition of g2d_lock and g2d_unlock lock macros	http://security.samsungmobile.com/smrupdate.html#SMR-OCT-2015	O-SAM-SAMSU-140817/210

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

			as no-ops, aka SVE-2015-4598. **CVE-2015-7891**		
Sol-connect					
Sol.connect Iset-mpp Meter Firmware					
Exec Code Sql	2017-08-02	7.5	SQL injection vulnerability in SOL.Connect ISET-mpp meter 1.2.4.2 and earlier allows remote attackers to execute arbitrary SQL commands via the user parameter in a login action. **CVE-2017-11494**	NA	O-SOL-SOL.C-140817/211
Technicolor					
Tc7337 Firmware					
XSS	2017-08-03	4.3	Persistent XSS through the SSID of nearby Wi-Fi devices on Technicolor TC7337 routers 08.89.17.20.00 allows an attacker to cause DNS Poisoning and steal credentials from the router. **CVE-2017-11320**	NA	O-TEC-TC733-140817/212
Operating System; Application (OS/A)					
Fedoraproject;Opensuse Project/Jasper Project					
Fedora/Leap;Opensuse/Jasper					
DoS	2017-08-02	4.3	Double free vulnerability in the jasper_image_stop_load function in JasPer 1.900.17 allows remote attackers to cause a denial of service (crash) via a crafted JPEG 2000 image file. **CVE-2015-5203**	https://bugzilla.redhat.com/show_bug.cgi?id=1254242	O-FED-FEDOR-140817/213

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