Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/ Patch	NCIIPCID
Application					
2345 Security Guard Project					
2345 Security Guard					
DoS	18-03-2018	6.1	In 2345 Security Guard 3.6, the driver file (2345NetFirewall.sys) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0x00222018. **CVE-ID:CVE-2018-8765**	href=https://github.com/D0neMkj/POC_BSOD/tree/master/2345%20security%20guard/0x00222018	A-234-2345/16-04-18/01
DoS	20-03-2018	6.1	In 2345 Security Guard 3.6, the driver file (2345NetFirewall.sys) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0x00222040. **CVE-ID:CVE-2018-8873**	href=https://github.com/D0neMkj/POC_BSOD/tree/master/2345%20security%20guard/0x00222040	A-234-2345/16-04-18/02
DoS	20-03-2018	6.1	In 2345 Security Guard 3.6, the driver file (2345Wrath.sys) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0x00222054. **CVE-ID:CVE-2018-8874**	href=https://github.com/D0neMkj/POC_BSOD/tree/master/2345%20security%20guard/0x00222054	A-234-2345/16-04-18/03
DoS	20-03-2018	6.1	In 2345 Security Guard 3.6, the driver file (2345Wrath.sys) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0x00222098. **CVE-ID:CVE-2018-8876**	href=https://github.com/D0neMkj/POC_BSOD/tree/master/2345%20security%20guard/0x00222098	A-234-2345/16-04-18/04

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/ Patch	NCIIPCID
DoS	20-03-2018	6.1	In 2345 Security Guard 3.6, the driver file (2345Wrath.sys) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0x0022209c. **CVE-ID:CVE-2018-8875**	href=https://github.com/D0neMkj/POC_BSOD/tree/master/2345%20security%20guard/0x0022209c	A-234-2345/16-04-18/05
DoS	22-03-2018	6.1	In 2345 Security Guard 3.6, the driver file (2345BdPcSafe.sys) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0x00222108. **CVE-ID:CVE-2018-8894**	href=https://github.com/D0neMkj/POC_BSOD/tree/master/2345%20security%20guard/0x00222108	A-234-2345/16-04-18/06
DoS	22-03-2018	6.1	In 2345 Security Guard 3.6, the driver file (2345DumpBlock.sys) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0x00222040. **CVE-ID:CVE-2018-8895**	href=https://github.com/D0neMkj/POC_BSOD/tree/master/2345%20security%20guard/2345DumpBlock.sys-0x00222040	A-234-2345/16-04-18/07
DoS	22-03-2018	6.1	In 2345 Security Guard 3.6, the driver file (2345DumpBlock.sys) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0x00222044. **CVE-ID:CVE-2018-8896**	href=https://github.com/D0neMkj/POC_BSOD/tree/master/2345%20security%20guard/2345DumpBlock.sys-0x00222044	A-234-2345/16-04-18/08

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/ Patch	NCIIPCID
Alkacon					
Opencms					
CSRF	20-03-2018	6.8	Cross-site request forgery (CSRF) vulnerability in system/workplace /admin/accounts/user_role.jsp in OpenCMS 10.5.3 allows remote attackers to hijack the authentication of administrative users for requests that perform privilege escalation. **CVE-ID:CVE-2018-8811**	href=https://github.com/alkacon/opencms-core/issues/586,href=https://www.exploit-db.com/exploits/44391/	A-Alk-Openc/16-04-18/09
XSS	20-03-2018	3.5	Cross-site scripting (XSS) vulnerability in the gallery function in Alkacon OpenCMS 10.5.3 allows remote attackers to inject arbitrary web script or HTML via a malicious SVG image. **CVE-ID:CVE-2018-8815**	href=https://github.com/alkacon/opencms-core/issues/587,href=https://www.exploit-db.com/exploits/44392/	A-Alk-Openc/16-04-18/10
Artezio					
Kanban Board					
XSS	16-03-2018	3.5	The Artezio Kanban Board plugin 1.4 revision 1914 for Atlassian Jira has XSS via the Board Name in a Create New Board action, related to an artezioboard/mainPage.jspa?kanbanId=7#/kanban-view URI. **CVE-ID:CVE-2016-10715**	href=https://packetstormsecurity.com/files/137648/JIRA-Artezio-Board-1.4-Cross-Site-Scripting-Information-Disclosure.html	A-Art-Kanba/16-04-18/11
Bylancer					
Bookme					
XSS	17-03-2018	3.5	Bookme Control Panel 2.0 Application is vulnerable to stored XSS within the Customers "Book Me" function. Within the Name and Note (aka custName and custNote) sections of the Customers screen, the application does not sanitize user-supplied input and renders injected JavaScript code to the user's browser. **CVE-ID:CVE-2018-8737**	href=https://neetech18.blogspot.in/2018/03/stored-xss-vulnerability-in-bookme_17.html	A-Byl-Bookm/16-04-18/12

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/ Patch	NCIIPCID
Cacti					
Cacti					
XSS	12-04-2018	3.5	Cacti before 1.1.37 has XSS because it does not properly reject unintended characters, related to use of the sanitize_uri function in lib/functions.php. **CVE-ID:CVE-2018-10060**	href=https://github.com/Cacti/cacti/issues/1457,href=https://www.cacti.net/changelog.php	A-Cac-Cacti/16-04-18/13
XSS	12-04-2018	3.5	Cacti before 1.1.37 has XSS because it makes certain htmlspecialchars calls without the ENT_QUOTES flag (these calls occur when the html_escape function in lib/html.php is not used). **CVE-ID:CVE-2018-10061**	href=https://github.com/Cacti/cacti/issues/1457,href=https://www.cacti.net/changelog.php	A-Cac-Cacti/16-04-18/14
Cmsmadesimple					
Cms Made Simple					
Bypass	13-04-2018	6.5	CMS Made Simple (CMSMS) through 2.2.6 contains a privilege escalation vulnerability from ordinary user to admin user by arranging for the eff_uid value within $_COOKIE[$this->_loginkey] to equal 1, because an SHA-1 cryptographic protection mechanism can be bypassed. **CVE-ID:CVE-2018-10084**	href=https://github.com/itodaro/cve/blob/master/README.md	A-Cms-Cms/16-04-18/15
CSRF	11-04-2018	6.8	CMS Made Simple (aka CMSMS) 2.2.7 has CSRF in admin/moduleinterface.php. **CVE-ID:CVE-2018-**10031	href=https://github.com/zxyxx/cmsms_vul	A-Cms-Cms/16-04-18/16
CSRF	11-04-2018	6.8	CMS Made Simple (aka CMSMS) 2.2.7 has CSRF in admin/siteprefs.php. **CVE-ID:CVE-2018-10030**	href=https://github.com/zxyxx/cmsms_vul	A-Cms-Cms-16-04-18/17

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/ Patch	NCIIPCID
Directory Traversal	13-04-2018	6.4	CMS Made Simple (CMSMS) through 2.2.7 contains an arbitrary file deletion vulnerability in the admin dashboard via directory traversal sequences in the val parameter within a cmd=del request, because code under modules\FilePicker does not restrict the val parameter. **CVE-ID:CVE-2018-10083**	href=https://github.com/itodaro/cve/blob/master/README.md	A-Cms-Cms/16-04-18/18
Execute Code	13-04-2018	7.5	CMS Made Simple (CMSMS) through 2.2.6 allows PHP object injection because of an unserialize call in the _get_data function of \lib\classes\internal\class.LoginOperations.php. By sending a crafted cookie, a remote attacker can upload and execute code, or delete files. **CVE-ID:CVE-2018-10085**	href=https://github.com/itodaro/cve/blob/master/README.md	A-Cms-Cms/16-04-18/19
Execute Code Bypass	13-04-2018	6.5	CMS Made Simple (CMSMS) through 2.2.7 contains an arbitrary code execution vulnerability in the admin dashboard because the implementation uses "eval('function testfunction'.rand()" and it is possible to bypass certain restrictions on these "testfunction" functions. **CVE-ID:CVE-2018-10086**	href=https://github.com/itodaro/cve/blob/master/README.md	A-Cms-Cms/16-04-18/20

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/ Patch	NCIIPCID
Gain Informatyion	13-04-2018	5	CMS Made Simple (CMSMS) through 2.2.7 allows physical path leakage via an invalid /index.php?page= value, a crafted URI starting with /index.php?mact=Search, or a direct request to /admin/header.php, /admin/footer.php, /lib/tasks/class.ClearCache.task.php, or /lib/tasks/class.CmsSecurityCheck.task.php. **CVE-ID:CVE-2018-10082**	href=https://github.com/itodaro/cve/blob/master/README.md	A-Cms-Cms/16-04-18/21
XSS	11-04-2018	3.5	CMS Made Simple (aka CMSMS) 2.2.7 has Reflected XSS in admin/moduleinterface.php via the m1_name parameter, related to moduledepends, a different vulnerability than CVE-2017-16799. **CVE-ID:CVE-2018-10029**	href=https://github.com/zxyxx/cms ms_vul	A-Cms-Cms/16-04-18/22
XSS	11-04-2018	3.5	CMS Made Simple (aka CMSMS) 2.2.7 has Reflected XSS in admin/moduleinterface.php via the m1_version parameter. **CVE-ID:CVE-2018-**10032	href=https://github.com/zxyxx/cms ms_vul	A-Cms-Cms/16-04-18/23
XSS	11-04-2018	3.5	CMS Made Simple (aka CMSMS) 2.2.7 has Stored XSS in admin/siteprefs.php via the metadata parameter. **CVE-ID:CVE-2018-10033**	href=https://github.com/zxyxx/cms ms_vul	A-Cms-Cms/16-04-18/24

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/ Patch	NCIIPCID
Coppermine-gallery					
Coppermine Photo Gallery					
XSS	16-03-2018	4.3	Cross-site scripting (XSS) vulnerability in the keywords manager (keywordmgr.php) in Coppermine Photo Gallery before 1.5.27 and 1.6.x before 1.6.01 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors. **CVE-ID:CVE-2014-4612**	href=https://sourceforge.net/p/coppermine/code/8674/tree//trunk/cpg1.5.x/CHANGELOG.txt,href=https://sourceforge.net/p/coppermine/code/8674/tree//trunk/cpg1.6.x/CHANGELOG.txt	A-Cop-Coppe/16-04-18/25
Docutracinc					
Dtisqlinstaller					
	19-03-2018	10	Versions of DocuTrac QuicDoc and Office Therapy that ship with DTISQLInstaller.exe version 1.6.4.0 and prior contain three credentials with known passwords: QDMaster, OTMaster, and sa. **CVE-ID:CVE-2018-5551**	href=https://blog.rapid7.com/2018/03/14/r7-2018-01-cve-2018-5551-cve-2018-5552-docutrac-office-therapy-installer-hard-coded-credentials-and-cryptographic-salt/	A-Doc-Dtisq-16-04-18/26

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/ Patch	NCIIPCID
EMC					
Data Protection Advisor					
Gain Privileges	16-03-2018	7.5	EMC Data Protection Advisor 6.3.x before patch 67 and 6.4.x before patch 130 contains undocumented accounts with hard-coded passwords and various privileges. Affected accounts are: "Apollo System Test", "emc.dpa.agent.logon" and "emc.dpa.metrics.logon". An attacker with knowledge of the password could potentially use these accounts via REST APIs to gain unauthorized access to EMC Data Protection Advisor (including potentially access with administrative privileges). **CVE-ID:CVE-2017-8013**	NA	A-EMC-Data/16-04-18/27
Gitlab					
Gitlab					
NA	21-03-2018	4	Gitlab Community Edition version 10.3 is vulnerable to an improper authorization issue in the deployment keys component resulting in unauthorized use of deployment keys by guest users. **CVE-ID:CVE-2017-0927**	href=https://gitlab.com/gitlab-org/gitlab-ce/issues/37594,href=https://about.gitlab.com/2018/01/16/gitlab-10-dot-3-dot-4-released/	A-Git-Gitla/16-04-18/28
XSS	21-03-2018	4.3	Gitlab Community Edition version 10.2.4 is vulnerable to lack of input validation in the labels component resulting in persistent cross site scripting. **CVE-ID:CVE-2017-0924**	href=https://hackerone.com/reports/294099,href=https://about.gitlab.com/2018/01/16/gitlab-10-dot-3-dot-4-released/	A-Git-Gitla/16-04-18/ 29

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/ Patch	NCIIPCID
XSS	21-03-2018	4.3	Gitlab Community Edition version 9.1 is vulnerable to lack of input validation in the IPython notebooks component resulting in persistent cross site scripting. **CVE-ID:CVE-2017-0923**	href=https://hackerone.com/reports/293740,href=https://about.gitlab.com/2018/01/16/gitlab-10-dot-3-dot-4-released/	A-Git-Gitla/16-04-18/ 30
IBM					
Connections					
DoS	20-03-2018	4	XML external entity (XXE) vulnerability in IBM Connections 3.0.1.1 and earlier, 4.0, 4.5, and 5.0 before CR4 allows remote authenticated users to cause a denial of service (memory consumption) via crafted XML data. IBM X-Force ID: 108357. **CVE-ID:CVE-2015-7461**	href=https://exchange.xforce.ibmcloud.com/vulnerabilities/108357	A-IBM-Conne/16-04-18/31
XSS	20-03-2018	3.5	Cross-site scripting (XSS) vulnerability in IBM Connections 3.0.1.1 and earlier, 4.0, 4.5, and 5.0 before CR4 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors. IBM X-Force ID: 108354. **CVE-ID:CVE-2015-7458**	href=https://exchange.xforce.ibmcloud.com/vulnerabilities/108354	A-IBM-Conne/16-04-18/32
XSS	20-03-2018	3.5	Cross-site scripting (XSS) vulnerability in IBM Connections 3.0.1.1 and earlier, 4.0, 4.5, and 5.0 before CR4 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors. IBM X-Force ID: 108355. **CVE-ID:CVE-2015-7459**	href=https://exchange.xforce.ibmcloud.com/vulnerabilities/108355	A-IBM-Conne/16-04-18/33

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/ Patch	NCIIPCID
XSS	20-03-2018	3.5	Cross-site scripting (XSS) vulnerability in IBM Connections 3.0.1.1 and earlier, 4.0, 4.5, and 5.0 before CR4 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors. IBM X-Force ID: 108356. **CVE-ID:CVE-2015-7460**	href=https://exchange.xforce.ibmcloud.com/vulnerabilities/108356	A-IBM-Conne/16-04-18/34
Rational Collaborative Lifecycle Management,Rational Doors Next Generation,Rational Engineering Lifecycle Manager,Rational Quality Manager,Rational Rhapsody Design Manager,Rational Software Architect Design Manager,Rational Team Concert					
XSS	23-03-2018	3.5	IBM Jazz Foundation (IBM Rational Collaborative Lifecycle Management 5.0 and 6.0) 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: 133127. **CVE-ID:CVE-2017-1629**	href=https://exchange.xforce.ibmcloud.com/vulnerabilities/133127	A-IBM-Ratio/16-04-18/35
XSS	23-03-2018	3.5	IBM Jazz Foundation (IBM Rational Collaborative Lifecycle Management 5.0 and 6.0) 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: 133379. **CVE-ID:CVE-2017-1655**	href=https://exchange.xforce.ibmcloud.com/vulnerabilities/133379	A-IBM-Ratio/16-04-18/36

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/ Patch	NCIIPCID
XSS	23-03-2018	3.5	IBM Jazz Foundation (IBM Rational Collaborative Lifecycle Management 5.0 and 6.0) 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: 136006. **CVE-ID:CVE-2017-1762**	href=https://exchange.xforce.ibmcloud.com/vulnerabilities/136006	A-IBM-Ratio/16-04-18/37
I-librarian					
I Librarian					
NA	23-03-2018	6.4	I, Librarian version 4.8 and earlier contains a SSRF vulnerability in "url" parameter of getFromWeb in functions.php that can result in the attacker abusing functionality on the server to read or update internal resources. **CVE-ID:CVE-2018-1000138**	href=https://github.com/mkucej/i-librarian/issues/120,href=https://github.com/mkucej/i-librarian/blob/9535753a84bc615b210802d4c9542db73368d984/functions.php#L811	A-I-l-I/16-04-18/38
CSRF	23-03-2018	6.8	I, Librarian version 4.8 and earlier contains a Cross site Request Forgery (CSRF) vulnerability in users.php that can result in the password of the admin being forced to be changed without the administrator's knowledge. **CVE-ID:CVE-2018-1000137**	href=https://github.com/mkucej/i-librarian/issues/121	A-I-l-I/16-04-18/39
XSS	23-03-2018	4.3	I, Librarian version 4.8 and earlier contains a Cross Site Scripting (XSS) vulnerability in "id" parameter in stable.php that can result in an attacker using the XSS to send a malicious script to an unsuspecting user. **CVE-ID:CVE-2018-1000139**	href=https://github.com/mkucej/i-librarian/issues/119,href=https://github.com/mkucej/i-librarian/blob/9535753a84bc615b210802d4c9542db73368d984/stable.php#L8	A-I-l-I/16-04-18/40

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/ Patch	NCIIPCID
Imagemagick					
Imagemagick					
DoS	20-03-2018	6.8	WriteEPTImage in coders/ept.c in ImageMagick 7.0.7-25 Q16 allows remote attackers to cause a denial of service (MagickCore/memory.c double free and application crash) or possibly have unspecified other impact via a crafted file. **CVE-ID:CVE-2018-8804**	href=https://github.com/ImageMagick/ImageMagick/issues/1025	A-Ima-Image/16-04-18/41
DoS	26-03-2018	4.3	An issue was discovered in ImageMagick 7.0.7. A memory leak vulnerability was found in the function ReadPCDImage in coders/pcd.c, which allow remote attackers to cause a denial of service via a crafted file. **CVE-ID:CVE-2017-18251**	href=https://github.com/ImageMagick/ImageMagick/issues/809	A-Ima-Image/16-04-18/42
DoS	26-03-2018	4.3	An issue was discovered in ImageMagick 7.0.7. A memory leak vulnerability was found in the function WriteGIFImage in coders/gif.c, which allow remote attackers to cause a denial of service via a crafted file. **CVE-ID:CVE-2017-18254**	href=https://github.com/ImageMagick/ImageMagick/issues/808	A-Ima-Image/16-04-18/43
DoS	26-03-2018	4.3	An issue was discovered in ImageMagick 7.0.7. A NULL pointer dereference vulnerability was found in the function LoadOpenCLDevices in MagickCore/opencl.c, which allows attackers to cause a denial of service via a crafted file. **CVE-ID:CVE-2017-18253**	href=https://github.com/ImageMagick/ImageMagick/issues/794	A-Ima-Image/16-04-18/44

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/ Patch	NCIIPCID
DoS	26-03-2018	4.3	An issue was discovered in ImageMagick 7.0.7. A NULL pointer dereference vulnerability was found in the function LogOpenCLBuildFailure in MagickCore/opencl.c, which allows attackers to cause a denial of service via a crafted file. **CVE-ID:CVE-2017-18250**	href=https://github.com/ImageMagick/ImageMagick/issues/793	A-Ima-Image/16-04-18/45
DoS	26-03-2018	4.3	An issue was discovered in ImageMagick 7.0.7. The MogrifyImageList function in MagickWand/mogrify.c allows attackers to cause a denial of service (assertion failure and application exit in ReplaceImageInList) via a crafted file. **CVE-ID:CVE-2017-18252**	href=https://github.com/ImageMagick/ImageMagick/issues/802	A-Ima-Image/16-04-18/46
Overflow	23-03-2018	6.8	The ReadTIFFImage function in coders/tiff.c in ImageMagick 7.0.7-26 Q16 does not properly restrict memory allocation, leading to a heap-based buffer over-read. **CVE-ID:CVE-2018-8960**	href=https://github.com/ImageMagick/ImageMagick/issues/1020	A-Ima-Image/16-04-18/47
Iobit					
Advanced Systemcare Ultimate					
DoS	24-03-2018	6.1	In Advanced SystemCare Ultimate 11.0.1.58, the driver file (Monitor_win7_x64.sys) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0x9c402000. **CVE-ID:CVE-2018-9001**	href=https://github.com/D0neMkj/POC_BSOD/tree/master/Advanced%20SystemCare%20Utimate/Monitor_win7_x64.sys-0x9c402000	A-Iob-Advan/16-04-18/48

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/ Patch	NCIIPCID
DoS	24-03-2018	6.1	In Advanced SystemCare Ultimate 11.0.1.58, the driver file (Monitor_win7_x64.sys) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0x9c402004. **CVE-ID:CVE-2018-9006**	href=https://github.com/D0neMkj/POC_BSOD/tree/master/Advanced%20SystemCare%20Utimate/Monitor_win7_x64.sys-0x9c402004	A-Iob-Advan/16-04-18/49
DoS	24-03-2018	6.1	In Advanced SystemCare Ultimate 11.0.1.58, the driver file (Monitor_win7_x64.sys) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0x9c4060c4. **CVE-ID:CVE-2018-8999**	href=https://github.com/D0neMkj/POC_BSOD/tree/master/Advanced%20SystemCare%20Utimate/Monitor_win7_x64.sys-0x9c4060c4	A-Iob-Advan/16-04-18/50
DoS	24-03-2018	6.1	In Advanced SystemCare Ultimate 11.0.1.58, the driver file (Monitor_win7_x64.sys) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0x9c4060cc. **CVE-ID:CVE-2018-9002**	href=https://github.com/D0neMkj/POC_BSOD/tree/master/Advanced%20SystemCare%20Utimate/Monitor_win7_x64.sys-0x9c4060cc	A-Iob-Advan/16-04-18/51
DoS	24-03-2018	6.1	In Advanced SystemCare Ultimate 11.0.1.58, the driver file (Monitor_win7_x64.sys) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0x9c4060d0. **CVE-ID:CVE-2018-9005**	href=https://github.com/D0neMkj/POC_BSOD/tree/master/Advanced%20SystemCare%20Utimate/Monitor_win7_x64.sys-0x9c4060d0	A-Iob-Advan/16-04-18/52

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/ Patch	NCIIPCID
DoS	24-03-2018	6.1	In Advanced SystemCare Ultimate 11.0.1.58, the driver file (Monitor_x86.sys) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0x9c402000. **CVE-ID:CVE-2018-9003**	href=https://github.com/D0neMkj/POC_BSOD/tree/master/Advanced%20SystemCare%20Utimate/Monitor_win7_x86.sys-0x9c402000	A-Iob-Advan/16-04-18/53
DoS	24-03-2018	6.1	In Advanced SystemCare Ultimate 11.0.1.58, the driver file (Monitor_x86.sys) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0x9c402004. **CVE-ID:CVE-2018-9000**	href=https://github.com/D0neMkj/POC_BSOD/tree/master/Advanced%20SystemCare%20Utimate/Monitor_win7_x86.sys-0x9c402004	A-Iob-Advan/16-04-18/54
DoS	24-03-2018	6.1	In Advanced SystemCare Ultimate 11.0.1.58, the driver file (Monitor_x86.sys) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0x9c4060c4. **CVE-ID:CVE-2018-9007**	href=https://github.com/D0neMkj/POC_BSOD/tree/master/Advanced%20SystemCare%20Utimate/Monitor_win7_x86.sys-0x9c4060c4	A-Iob-Advan/16-04-18/55
DoS	24-03-2018	6.1	In Advanced SystemCare Ultimate 11.0.1.58, the driver file (Monitor_x86.sys) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0x9c4060cc. **CVE-ID:CVE-2018-8998**	href=https://github.com/D0neMkj/POC_BSOD/tree/master/Advanced%20SystemCare%20Utimate/Monitor_win7_x86.sys-0x9c4060cc	A-Iob-Advan/16-04-18/56
DoS	24-03-2018	6.1	In Advanced SystemCare Ultimate 11.0.1.58, the driver file (Monitor_x86.sys) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0x9c4060d0. **CVE-ID:CVE-2018-9004**	href=https://github.com/D0neMkj/POC_BSOD/tree/master/Advanced%20SystemCare%20Utimate/Monitor_win7_x86.sys-0x9c4060d0	A-Iob-Advan/16-04-18/57

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/ Patch	NCIIPCID
DoS	26-03-2018	6.1	In Advanced SystemCare Ultimate 11.0.1.58, the driver file (Monitor_win10_x64.sys) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0x9c402000. **CVE-ID:CVE-2018-9042**	href=https://github.com/D0neMkj/POC_BSOD/tree/master/Advanced%20SystemCare%20Utimate/Monitor_win10_x64.sys-0x9c402000	A-Iob-Advan/16-04-18/58
DoS	26-03-2018	6.1	In Advanced SystemCare Ultimate 11.0.1.58, the driver file (Monitor_win10_x64.sys) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0x9c402004. **CVE-ID:CVE-2018-9041**	href=https://github.com/D0neMkj/POC_BSOD/tree/master/Advanced%20SystemCare%20Utimate/Monitor_win10_x64.sys-0x9c402004	A-Iob-Advan/16-04-18/59
DoS	26-03-2018	6.1	In Advanced SystemCare Ultimate 11.0.1.58, the driver file (Monitor_win10_x64.sys) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0x9c4060c4. **CVE-ID:CVE-2018-9040**	href=https://github.com/D0neMkj/POC_BSOD/tree/master/Advanced%20SystemCare%20Utimate/Monitor_win10_x64.sys-0x9c4060c4	A-Iob-Advan/16-04-18/60
DoS	26-03-2018	6.1	In Advanced SystemCare Ultimate 11.0.1.58, the driver file (Monitor_win10_x64.sys) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0x9c4060cc. **CVE-ID:CVE-2018-9044**	href=https://github.com/D0neMkj/POC_BSOD/tree/master/Advanced%20SystemCare%20Utimate/Monitor_win10_x64.sys-0x9c4060cc	A-Iob-Advan/16-04-18/61

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/ Patch	NCIIPCID
DoS	26-03-2018	6.1	In Advanced SystemCare Ultimate 11.0.1.58, the driver file (Monitor_win10_x64.sys) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0x9c4060d0. **CVE-ID:CVE-2018-9043**	href=https://github.com/D0neMkj/POC_BSOD/tree/master/Advanced%20SystemCare%20Utimate/Monitor_win10_x64.sys-0x9c4060d0	A-Iob-Advan/16-04-18/62
Jasper Project					
Jasper					
DoS	27-03-2018	4.3	JasPer 2.0.14 allows denial of service via a reachable assertion in the function jpc_firstone in libjasper/jpc/jpc_math.c. **CVE-ID:CVE-2018-9055**	href=https://github.com/mdadams/jasper/issues/172	A-Jas-Jaspe/16-04-18/63
Joyplus-cms Project					
Joyplus-cms					
Execute Code	18-03-2018	7.5	joyplus-cms 1.6.0 allows Remote Code Execution because of an Arbitrary File Upload issue in manager/editor/upload.php, related to manager/admin_vod.php?action=add. **CVE-ID:CVE-2018-8766**	href=https://github.com/joyplus/joyplus-cms/issues/421	A-Joy-Joypl/16-04-18/64
XSS	18-03-2018	3.5	joyplus-cms 1.6.0 has XSS in manager/admin_ajax.php?action=save&tab={pre}vod_type via the t_name parameter. **CVE-ID:CVE-2018-8767**	href=https://github.com/joyplus/joyplus-cms/issues/420	A-Joy-Joypl/16-04-18/65
Jungo					
Windriver					
DoS	20-03-2018	7.1	Windrvr1260.sys in Jungo DriverWizard WinDriver 12.6.0 allows attackers to cause a denial of service (BSOD) via a crafted .exe file. **CVE-ID:CVE-2018-8821**	href=https://github.com/bigric3/poc	A-Jun-Windr/16-04-18/66

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/ Patch	NCIIPCID
Libav					
Libav					
DoS	23-03-2018	4.3	The av_audio_fifo_size function in libavutil/audio_fifo.c in Libav 12.2 allows remote attackers to cause a denial of service (NULL pointer dereference) via a crafted media file. **CVE-ID:CVE-2017-18247**	href=https://bugzilla.libav.org/show_bug.cgi?id=1089	A-Lib-Libav/16-04-18/67
DoS Overflow	23-03-2018	4.3	The mpc8_probe function in libavformat/mpc8.c in Libav 12.2 allows remote attackers to cause a denial of service (heap-based buffer over-read) via a crafted audio file. **CVE-ID:CVE-2017-18245**	href=https://bugzilla.libav.org/show_bug.cgi?id=1094	A-Lib-Libav/16-04-18/68
DoS Overflow	23-03-2018	4.3	The pcm_encode_frame function in libavcodec/pcm.c in Libav 12.2 allows remote attackers to cause a denial of service (heap-based buffer over-read) via a crafted media file. **CVE-ID:CVE-2017-18246**	href=https://bugzilla.libav.org/show_bug.cgi?id=1095	A-Lib-Libav/16-04-18/69
Libming					
Libming					
NA	20-03-2018	4.3	In libming 0.4.8, there is a use-after-free in the decompileArithmeticOp function of decompile.c. Remote attackers could use this vulnerability to cause a denial-of-service via a crafted swf file. **CVE-ID:CVE-2018-8806**	href=https://github.com/libming/libming/issues/128	A-Lib-Libmi/16-04-18/70
DoS	20-03-2018	4.3	In libming 0.4.8, these is a use-after-free in the function decompileCALLFUNCTION of decompile.c. Remote attackers could leverage this vulnerability to cause a denial of service via a crafted swf file. **CVE-ID:CVE-2018-8807**	href=https://github.com/libming/libming/issues/129	A-Lib-Libmi/16-04-18/71

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/ Patch	NCIIPCID
DoS	23-03-2018	4.3	In libming 0.4.8, the decompileDELETE function of decompile.c has a use-after-free. Remote attackers could leverage this vulnerability to cause a denial of service via a crafted swf file. **CVE-ID:CVE-2018-8964**	href=https://github.com/libming/libming/issues/130	A-Lib-Libmi/16-04-18/72
DoS	23-03-2018	4.3	In libming 0.4.8, the decompileGETVARIABLE function of decompile.c has a use-after-free. Remote attackers could leverage this vulnerability to cause a denial of service via a crafted swf file. **CVE-ID:CVE-2018-8963**	href=https://github.com/libming/libming/issues/130	A-Lib-Libmi/16-04-18/73
DoS	23-03-2018	4.3	In libming 0.4.8, the decompilePUSHPARAM function of decompile.c has a use-after-free. Remote attackers could leverage this vulnerability to cause a denial of service via a crafted swf file. **CVE-ID:CVE-2018-8961**	href=https://github.com/libming/libming/issues/130	A-Lib-Libmi/16-04-18/74
DoS	23-03-2018	4.3	In libming 0.4.8, the decompileSingleArgBuiltInFunctionCall function of decompile.c has a use-after-free. Remote attackers could leverage this vulnerability to cause a denial of service via a crafted swf file. **CVE-ID:CVE-2018-8962**	href=https://github.com/libming/libming/issues/130	A-Lib-Libmi/16-04-18/75
Libtiff					
Libtiff					
Overflow	22-03-2018	6.8	In LibTIFF 4.0.9, a heap-based buffer overflow occurs in the function LZWDecodeCompat in tif_lzw.c via a crafted TIFF file, as demonstrated by tiff2ps. **CVE-ID:CVE-2018-8905**	href=https://github.com/halfbitteam/POCs/tree/master/libtiff-4.08_tiff2ps_heaoverflow	A-Lib-Libti/16-04-18/ 76

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/ Patch	NCIIPCID
Nasm					
Netwide Assembler					
Overflow	20-03-2018	4.6	Netwide Assembler (NASM) 2.13.02rc2 has a buffer over-read in the parse_line function in asm/parser.c via uncontrolled access to nasm_reg_flags. **CVE-ID:CVE-2018-8883**	href=https://bugzilla.nasm.us/show_bug.cgi?id=3392447	A-Nas-Netwi/16-04-18/77
Overflow	20-03-2018	4.6	Netwide Assembler (NASM) 2.13.02rc2 has a heap-based buffer over-read in the function tokenize in asm/preproc.c, related to an unterminated string. **CVE-ID:CVE-2018-8881**	href=https://bugzilla.nasm.us/show_bug.cgi?id=3392446	A-Nas-Netwi/16-04-18/78
Overflow	20-03-2018	4.6	Netwide Assembler (NASM) 2.13.02rc2 has a stack-based buffer under-read in the function ieee_shr in asm/float.c via a large shift value. **CVE-ID:CVE-2018-8882**	href=https://bugzilla.nasm.us/show_bug.cgi?id=3392445	A-Nas-Netwi/16-04-18/79
Omron					
Cx-supervisor					
NA	21-03-2018	4.6	In Omron CX-Supervisor Versions 3.30 and prior, access of uninitialized pointer vulnerabilities can be exploited when CX Supervisor indirectly calls an initialized pointer when parsing malformed packets. **CVE-ID:CVE-2018-7515**	href=https://ics-cert.us-cert.gov/advisories/ICSA-18-072-01	A-Omr-Cx-su/16-04-18/80
NA	21-03-2018	4.6	In Omron CX-Supervisor Versions 3.30 and prior, parsing malformed project files may cause a double free vulnerability. **CVE-ID:CVE-2018-7523**	href=https://ics-cert.us-cert.gov/advisories/ICSA-18-072-01	A-Omr-Cx-su/16-04-18/81
NA	21-03-2018	4.6	In Omron CX-Supervisor Versions 3.30 and prior, parsing malformed project files may cause an out of bounds vulnerability. **CVE-ID:CVE-2018-7517**	href=https://ics-cert.us-cert.gov/advisories/ICSA-18-072-01	A-Omr-Cx-su/16-04-18/82

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/ Patch	NCIIPCID
NA	21-03-2018	4.6	In Omron CX-Supervisor Versions 3.30 and prior, processing a malformed packet by a certain executable may cause an untrusted pointer dereference vulnerability. **CVE-ID:CVE-2018-7525**	href=https://ics-cert.us-cert.gov/advisories/ICSA-18-072-01	A-Omr-Cx-su/16-04-18/83
NA	21-03-2018	4.6	In Omron CX-Supervisor Versions 3.30 and prior, use after free vulnerabilities can be exploited when CX Supervisor parses a specially crafted project file. **CVE-ID:CVE-2018-7521**	href=https://ics-cert.us-cert.gov/advisories/ICSA-18-072-01	A-Omr-Cx-su/16-04-18/84
Overflow	21-03-2018	4.6	In Omron CX-Supervisor Versions 3.30 and prior, parsing malformed project files may cause a heap-based buffer overflow. **CVE-ID:CVE-2018-7519**	href=https://ics-cert.us-cert.gov/advisories/ICSA-18-072-01	A-Omr-Cx-su/16-04-18/85
Overflow	21-03-2018	4.6	In Omron CX-Supervisor Versions 3.30 and prior, parsing malformed project files may cause a stack-based buffer overflow. **CVE-ID:CVE-2018-7513**	href=https://ics-cert.us-cert.gov/advisories/ICSA-18-072-01	A-Omr-Cx-su/16-04-18/86
Opendaylight					
Openflow					
NA	16-03-2018	7.5	OpenDayLight version Carbon SR3 and earlier contain a vulnerability during node reconciliation that can result in traffic flows that should be expired or should expire shortly being re-installed and their timers reset resulting in traffic being allowed that should be expired. **CVE-ID:CVE-2018-1078**	href=https://jira.opendaylight.org/browse/OPNFLWPLUG-971,href=https://bugzilla.redhat.com/show_bug.cgi?id=1533501	A-Ope-Openf/16-04-18/87
Openvpn					
Openvpn					
DoS Execute Code Gain Information	16-03-2018	6.4	** DISPUTED ** A cross-protocol scripting issue was discovered in the management interface in OpenVPN through	NA	A-Ope-Openv/16-04-18/88

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/ Patch	NCIIPCID
			2.4.5. When this interface is enabled over TCP without a password, and when no other clients are connected to this interface, attackers can execute arbitrary management commands, obtain sensitive information, or cause a denial of service (SIGTERM) by triggering XMLHttpRequest actions in a web browser. This is demonstrated by a multipart/form-data POST to http://localhost:23000 with a "signal SIGTERM" command in a TEXTAREA element. NOTE: The vendor disputes that this is a vulnerability. They state that this is the result of improper configuration of the Open VPN instance rather than an intrinsic vulnerability, and now more explicitly warn against such configurations in both the management-interface documentation, and with a runtime warning. **CVE-ID:CVE-2018-7544**		
Owncloud					
Owncloud					
XSS	20-03-2018	3.5	Cross-site scripting (XSS) vulnerability in own Cloud before 6.0.1 allows remote authenticated users to inject arbitrary web script or HTML via the filename of an uploaded file. **CVE-ID:CVE-2014-1665**	href=https://www.exploit-db.com/exploits/31427/,href=https://exchange.xforce.ibmcloud.com/vulnerabilities/91012,href=https://packetstormsecurity.com/files/125086	A-Own-Owncl/16-04-18/89

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/ Patch	NCIIPCID
Php 2chbbs Project					
Php 2chbbs					
XSS	22-03-2018	4.3	Cross-site scripting vulnerability in PHP 2chBBS version bbs18c allows an attacker to inject arbitrary web script or HTML via unspecified vectors. **CVE-ID:CVE-2018-0535**	href=https://jvn.jp/en/jp/JVN48774168/index.html	A-Php-Php/16-04-18/ 90
Pivotal Software					
Gemfire For Pivotal Cloud Foundry					
NA	16-03-2018	7.5	The GemFire broker for Cloud Foundry 1.6.x before 1.6.5 and 1.7.x before 1.7.1 has multiple API endpoints which do not require authentication and could be used to gain access to the cluster managed by the broker. **CVE-ID:CVE-2016-9880**	href=https://pivotal.io/security/cve-2016-9880	A-Piv-Gemfi/16-04-18/91

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/ Patch	NCIIPCID
Spring Framework,Spring Security					
Bypass	16-03-2018	5	Spring Security (Spring Security 4.1.x before 4.1.5, 4.2.x before 4.2.4, and 5.0.x before 5.0.1; and Spring Framework 4.3.x before 4.3.14 and 5.0.x before 5.0.3) does not consider URL path parameters when processing security constraints. By adding a URL path parameter with special encodings, an attacker may be able to bypass a security constraint. The root cause of this issue is a lack of clarity regarding the handling of path parameters in the Servlet Specification. Some Servlet containers include path parameters in the value returned for getPathInfo() and some do not. Spring Security uses the value returned by getPathInfo() as part of the process of mapping requests to security constraints. In this particular attack, different character encodings used in path parameters allows secured Spring MVC static resource URLs to be bypassed. **CVE-ID:CVE-2018-1199**	href=https://pivotal.io/security/cve-2018-1199	A-Piv-Sprin/16-04-18/92
Piwigo					
Piwigo					
CSRF	16-03-2018	4.3	Cross-site request forgery (CSRF) vulnerability in the administration panel in Piwigo before 2.6.2 allows remote attackers to hijack the authentication of administrators for requests that add users via a pwg.users.add action in a request to ws.php. **CVE-ID:CVE-2014-4613**		A-Piw-Piwig/16-04-18/93

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/ Patch	NCIIPCID
Qqq Systems Project					
Qqq Systems					
Execute Code	22-03-2018	10	QQQ SYSTEMS version 2.24 allows an attacker to execute arbitrary commands via unspecified vectors. **CVE-ID:CVE-2018-0539**	href=https://jvn.jp/en/jp/JVN22536871/index.html	A-Qqq/Qqq/16-04-18/94
XSS	22-03-2018	4.3	Cross-site scripting vulnerability in QQQ SYSTEMS ver2.24 allows an attacker to inject arbitrary web script or HTML via quiz.cgi. **CVE-ID:CVE-2018-0536**	href=https://jvn.jp/en/jp/JVN64990648/index.html	A-Qqq/Qqq/16-04-18/95
XSS	22-03-2018	4.3	Cross-site scripting vulnerability in QQQ SYSTEMS ver2.24 allows an attacker to inject arbitrary web script or HTML via quiz_op.cgi. **CVE-ID:CVE-2018-0537**	href=https://jvn.jp/en/jp/JVN96655441/index.html	A-Qqq/Qqq/16-04-18/96
Radare					
Radare2					
DoS Overflow	20-03-2018	4.3	In radare2 2.4.0, there is a heap-based buffer over-read in the dalvik_op function of anal_dalvik.c. Remote attackers could leverage this vulnerability to cause a denial of service via a crafted dex file. **CVE-ID:CVE-2018-8809**	href=https://github.com/radare/radare2/issues/9726	A-Rad-Radar/16-04-18/97
DoS Overflow	20-03-2018	4.3	In radare2 2.4.0, there is a heap-based buffer over-read in the get_ivar_list_t function of mach0_classes.c. Remote attackers could leverage this vulnerability to cause a denial of service via a crafted Mach-O file. **CVE-ID:CVE-2018-8810**	href=https://github.com/radare/radare2/issues/9727	A-Rad-Radar/16-04-18/98
DoS Overflow	20-03-2018	4.3	In radare2 2.4.0, there is a heap-based buffer over-read in the r_asm_disassemble function of asm.c. Remote attackers could leverage this vulnerability to cause a denial of service via a crafted dex file. **CVE-ID:CVE-2018-8808**	href=https://github.com/radare/radare2/issues/9725	A-Rad-Radar/16-04-18/99

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/ Patch	NCIIPCID
Secluded					
Trident					
Gain Privileges	16-03-2018	6	Pitchfork version 1.4.6 RC1 contains an Improper Privilege Management vulnerability in Trident Pitchfork components that can result in A standard unprivileged user could gain system administrator permissions within the web portal.. This attack appear to be exploitable via The user must be able to login, and could edit their profile and set the "System Administrator" permission to "yes" on themselves.. This vulnerability appears to have been fixed in 1.4.6 RC2. **CVE-ID:CVE-2018-1000133**	href=https://github.com/tridentli/pitchfork/commit/33549f15707801099e1253dd5e79369bd48eb59b,href=https://github.com/tridentli/trident/releases/tag/DEV_1.4.6-RC2,href=https://thomas-ward.net/security-advisories/trident-trusted-communications-platform-privilege-escalation-issue-advisory/,href=https://github.com/tridentli/pitchfork/issues/168,href=https://github.com/tridentli/pitchfork/commit/9fd07cbe4f93e1367e142016e9a205366680dd54	A-Sec-Tride/16-04-18/ 100
Sqlite					
Sqlite					
NA	16-03-2018	5	In SQLite through 3.22.0, databases whose schema is corrupted using a CREATE TABLE AS statement could cause a NULL pointer dereference, related to build.c and prepare.c. **CVE-ID:CVE-2018-8740**	href=https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=6964,href=https://bugs.launchpad.net/ubuntu/+source/sqlite3/+bug/1756349,href=https://www.sqlite.org/cgi/src/timeline?r=corrupt-	A-Sql-Sqlit/16-04-18/ 101

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/ Patch	NCIIPCID
				schema,href=https://www.sqlite.org/cgi/src/vdiff?from=1774f1c3baf0bc3d&to=d75e67654aa9620b	
Wampserver					
Wampserver					
XSS	19-03-2018	3.5	Cross-site scripting (XSS) vulnerability in WampServer 3.1.1 allows remote attackers to inject arbitrary web script or HTML via the virtual_del parameter. **CVE-ID:CVE-2018-8732**	href=https://www.exploit-db.com/exploits/44384/	A-Wam-Wamps/16-04-18/ 102
Webproxy Project					
Webproxy					
Directory Traversal	22-03-2018	5	Directory traversal vulnerability in WebProxy version 1.7.8 allows an attacker to read arbitrary files via unspecified vectors. **CVE-ID:CVE-2018-0542**	href=https://jvn.jp/en/jp/JVN87226910/index.html	A-Web-Webpr/16-04-18/ 103
Windows Optimization Master Project					
Windows Optimization Master					
DoS	22-03-2018	6.1	In Windows Master (aka Windows Optimization Master) 7.99.13.604, the driver file (WoptiHWDetect.SYS) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0xf1002000. **CVE-ID:CVE-2018-8904**	href=https://github.com/D0neMkj/POC_BSOD/tree/master/Windows%20Optimization%20master/0xf1002000	A-Win-Windo/16-04-18/104
DoS	24-03-2018	6.1	In Windows Master (aka Windows Optimization Master) 7.99.13.604, the driver file (WoptiHWDetect.SYS) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0xf1002001. **CVE-ID:CVE-2018-8993**	href=https://github.com/D0neMkj/POC_BSOD/tree/master/Windows%20Optimization%20master/0xf1002001	A-Win-Windo/16-04-18/105

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/ Patch	NCIIPCID
DoS	24-03-2018	6.1	In Windows Master (aka Windows Optimization Master) 7.99.13.604, the driver file (WoptiHWDetect.SYS) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0xf1002002. **CVE-ID:CVE-2018-8995**	href=https://github.com/D0neMkj/POC_BSOD/tree/master/Windows%20Optimization%20master/0xf1002002	A-Win-Windo/16-04-18/106
DoS	24-03-2018	6.1	In Windows Master (aka Windows Optimization Master) 7.99.13.604, the driver file (WoptiHWDetect.SYS) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0xf1002003. **CVE-ID:CVE-2018-8994**	href=https://github.com/D0neMkj/POC_BSOD/tree/master/Windows%20Optimization%20master/0xf1002003	A-Win-Windo/16-04-18/107
DoS	24-03-2018	6.1	In Windows Master (aka Windows Optimization Master) 7.99.13.604, the driver file (WoptiHWDetect.SYS) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0xf1002004. **CVE-ID:CVE-2018-8997**	href=https://github.com/D0neMkj/POC_BSOD/tree/master/Windows%20Optimization%20master/0xf1002004	A-Win-Windo/16-04-18/108
DoS	24-03-2018	6.1	In Windows Master (aka Windows Optimization Master) 7.99.13.604, the driver file (WoptiHWDetect.SYS) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0xf1002005. **CVE-ID:CVE-2018-8992**	href=https://github.com/D0neMkj/POC_BSOD/tree/master/Windows%20Optimization%20master/0xf1002005	A-Win-Windo/16-04-18/109

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/ Patch	NCIIPCID
DoS	24-03-2018	6.1	In Windows Master (aka Windows Optimization Master) 7.99.13.604, the driver file (WoptiHWDetect.SYS) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0xf1002006. **CVE-ID:CVE-2018-8989**	href=https://github.com/D0neMkj/POC_BSOD/tree/master/Windows%20Optimization%20master/0xf1002006	A-Win-Windo/16-04-18/110
DoS	24-03-2018	6.1	In Windows Master (aka Windows Optimization Master) 7.99.13.604, the driver file (WoptiHWDetect.SYS) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0xf1002007. **CVE-ID:CVE-2018-8996**	href=https://github.com/D0neMkj/POC_BSOD/tree/master/Windows%20Optimization%20master/0xf1002007	A-Win-Windo/16-04-18/111
DoS	24-03-2018	6.1	In Windows Master (aka Windows Optimization Master) 7.99.13.604, the driver file (WoptiHWDetect.SYS) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0xf1002008. **CVE-ID:CVE-2018-8988**	href=https://github.com/D0neMkj/POC_BSOD/tree/master/Windows%20Optimization%20master/0xf1002008	A-Win-Windo/16-04-18/112
DoS	24-03-2018	6.1	In Windows Master (aka Windows Optimization Master) 7.99.13.604, the driver file (WoptiHWDetect.SYS) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0xf1002009. **CVE-ID:CVE-2018-8991**	href=https://github.com/D0neMkj/POC_BSOD/tree/master/Windows%20Optimization%20master/0xf1002009	A-Win-Windo/16-04-18/113

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/ Patch	NCIIPCID
DoS	24-03-2018	6.1	In Windows Master (aka Windows Optimization Master) 7.99.13.604, the driver file (WoptiHWDetect.SYS) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0xf1002010. **CVE-ID:CVE-2018-8990**	href=https://github.com/D0neMkj/POC_BSOD/tree/master/Windows%20Optimization%20master/0xf1002010	A-Win-Windo/16-04-18/114
DoS	26-03-2018	6.1	In Windows Master (aka Windows Optimization Master) 7.99.13.604, the driver file (WoptiHWDetect.SYS) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0xf1002021. **CVE-ID:CVE-2018-9051**	href=https://github.com/D0neMkj/POC_BSOD/tree/master/Windows%20Optimization%20master/0xf1002021	A-Win-Windo/16-04-18/115
DoS	26-03-2018	6.1	In Windows Master (aka Windows Optimization Master) 7.99.13.604, the driver file (WoptiHWDetect.SYS) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0xf100202d. **CVE-ID:CVE-2018-9050**	href=https://github.com/D0neMkj/POC_BSOD/tree/master/Windows%20Optimization%20master/0xf10002D	A-Win-Windo/16-04-18/116
DoS	26-03-2018	6.1	In Windows Master (aka Windows Optimization Master) 7.99.13.604, the driver file (WoptiHWDetect.SYS) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0xf10026cc. **CVE-ID:CVE-2018-9053**	href=https://github.com/D0neMkj/POC_BSOD/tree/master/Windows%20Optimization%20master/0xf10026cc	A-Win-Windo/16-04-18/117

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/ Patch	NCIIPCID
DoS	26-03-2018	6.1	In Windows Master (aka Windows Optimization Master) 7.99.13.604, the driver file (WoptiHWDetect.SYS) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0xf100282c. **CVE-ID:CVE-2018-9048**	href=https://github.com/D0neMkj/POC_BSOD/tree/master/Windows%20Optimization%20master/0xf100282C	A-Win-Windo/16-04-18/118
DoS	26-03-2018	6.1	In Windows Master (aka Windows Optimization Master) 7.99.13.604, the driver file (WoptiHWDetect.SYS) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0xf100282d. **CVE-ID:CVE-2018-9046**	href=https://github.com/D0neMkj/POC_BSOD/tree/master/Windows%20Optimization%20master/0xf100282d	A-Win-Windo/16-04-18/119
DoS	26-03-2018	6.1	In Windows Master (aka Windows Optimization Master) 7.99.13.604, the driver file (WoptiHWDetect.SYS) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0xf1002833. **CVE-ID:CVE-2018-9049**	href=https://github.com/D0neMkj/POC_BSOD/tree/master/Windows%20Optimization%20master/0xf1002833	A-Win-Windo/16-04-18/120
DoS	26-03-2018	6.1	In Windows Master (aka Windows Optimization Master) 7.99.13.604, the driver file (WoptiHWDetect.SYS) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0xf100283c. **CVE-ID:CVE-2018-9052**	href=https://github.com/D0neMkj/POC_BSOD/tree/master/Windows%20Optimization%20master/0xf100283c	A-Win-Windo/16-04-18/121

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/ Patch	NCIIPCID
DoS	26-03-2018	6.1	In Windows Master (aka Windows Optimization Master) 7.99.13.604, the driver file (WoptiHWDetect.SYS) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0xf1002841. **CVE-ID:CVE-2018-9047**	href=https://github.com/D0neMkj/POC_BSOD/tree/master/Windows%20Optimization%20master/0xf1002841	A-Win-Windo/16-04-18/122
DoS	26-03-2018	6.1	In Windows Master (aka Windows Optimization Master) 7.99.13.604, the driver file (WoptiHWDetect.SYS) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0xf1002849. **CVE-ID:CVE-2018-9045**	href=https://github.com/D0neMkj/POC_BSOD/tree/master/Windows%20Optimization%20master/0xf1002849	A-Win-Windo/16-04-18/123
DoS	26-03-2018	6.1	In Windows Master (aka Windows Optimization Master) 7.99.13.604, the driver file (WoptiHWDetect.SYS) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0xf100284c. **CVE-ID:CVE-2018-9054**	href=https://github.com/D0neMkj/POC_BSOD/tree/master/Windows%20Optimization%20master/0xf100284c	A-Win-Windo/16-04-18/124
Yxcms					
Yxcms					
XSS	20-03-2018	4.3	Yxcms building system (compatible cell phone) v1.4.7 has XSS via the content parameter to protected\apps\default\view\default\extend_guestbook.php or protected\apps\default\view\mobile\extend_guestbook.php in an index.php?r=default/column/index&col=guestbook request. **CVE-ID:CVE-2018-8805**	href=https://github.com/QQ704568679/YXcms-Code-audit/blob/master/Yxcms%20Code%20audit	A-Yxc-Yxcms/16-04-18/125

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/ Patch	NCIIPCID
Application, Operating System (OS)					
Debian,Gitlab					
Debian Linux,Gitlab					
NA	21-03-2018	4	Gitlab Enterprise Edition version 10.1.0 is vulnerable to an insufficiently protected credential issue in the project service integration API endpoint resulting in an information disclosure of plaintext password. **CVE-ID:CVE-2017-0925**	href=https://www.debian.org/security/2018/dsa-4145,href=https://about.gitlab.com/2018/01/16/gitlab-10-dot-3-dot-4-released/,href=https://gitlab.com/gitlab-org/gitlab-ee/issues/3847	A-Deb-Debia/16-04-18/126
NA	21-03-2018	6.5	Gitlab Community Edition version 10.3 is vulnerable to an improper authorization issue in the Oauth sign-in component resulting in unauthorized user login. **CVE-ID:CVE-2017-0926**	href=https://www.debian.org/security/2018/dsa-4145,href=https://about.gitlab.com/2018/01/16/gitlab-10-dot-3-dot-4-released/,href=https://gitlab.com/gitlab-org/gitlab-ce/issues/32198	A-Deb-Debia/16-04-18/127
Debian,Squirrelmail					
Debian Linux,Squirrelmail					
Directory Traversal	17-03-2018	6.5	A directory traversal flaw in SquirrelMail 1.4.22 allows an authenticated attacker to exfiltrate (or potentially delete) files from the hosting server, related to../ In the att_local_name field in Deliver.class.php. **CVE-ID:CVE-2018-8741**	href=https://www.debian.org/security/2018/dsa-4168,href=https://gist.github.com/hannob/3c4f86863c418930ad08853c1109364e,href=https://insinuator.net/2018/03/squirrelmail-full-disclosure-troopers18/,href=https://paste.pound-python.org/show/OjSLiFTxiBrTk63jqEUu/	A-Deb-Debia/16-04-18/128

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/ Patch	NCIIPCID
Operating System (OS)					
Cisco					
Ios Xe					
NA	28-03-2018	4	A vulnerability in the web-based user interface (web UI) of Cisco IOS XE Software could allow an authenticated, remote attacker to write arbitrary files to the operating system of an affected device. The vulnerability is due to insufficient input validation of HTTP requests that are sent to the web UI of the affected software. An attacker could exploit this vulnerability by sending a malicious HTTP request to the web UI of the affected software. A successful exploit could allow the attacker to write arbitrary files to the operating system of an affected device. Cisco Bug IDs: CSCvb22645. **CVE-ID:CVE-2018-0196**	href=https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180328-wfw	O-Cis-Ios/16-04-18/129
Debian					
Debian Linux					
XSS	21-03-2018	4.3	Gitlab Community Edition version 10.2.4 is vulnerable to lack of input validation in the CI job component resulting in persistent cross site scripting. **CVE-ID:CVE-2017-0917**	href=https://www.debian.org/security/2018/dsa-4145,href=https://about.gitlab.com/2018/01/16/gitlab-10-dot-3-dot-4-released/,href=https://hackerone.com/reports/299525	O-Deb-Debia/16-04-18/130

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/ Patch	NCIIPCID
Google					
Android					
NA	16-03-2018	4.4	In Android for MSM, Firefox OS for MSM, QRD Android, with all Android releases from CAF using the Linux kernel, a race condition in diag_ioctl_lsm_deinit() leads to a Use After Free condition. **CVE-ID:CVE-2018-3561**	href=https://source.android.com/security/bulletin/pixel/2018-03-01	O-Goo-Andro/16-04-18/131
NA	16-03-2018	4.6	In Android for MSM, Firefox OS for MSM, QRD Android, with all Android releases from CAF using the Linux kernel, a Double Free vulnerability exists in Audio Driver while opening a sound compression device. **CVE-ID:CVE-2018-3560**	href=https://source.android.com/security/bulletin/pixel/2018-03-01	O-Goo-Andro/16-04-18/132
NA	16-03-2018	4.6	In Android for MSM, Firefox OS for MSM, QRD Android, with all Android releases from CAF using the Linux kernel, due to the lack of a range check on the array index into the WMI descriptor pool, arbitrary address execution may potentially occur in the process mgmt completion handler. **CVE-ID:CVE-2017-14889**	href=https://source.codeaurora.org/quic/la/platform/vendor/qcom-opensource/wlan/qcacld-3.0/commit/?id=e11e9dc8298dc0632050cacce96e9652d017f755,href=https://source.android.com/security/bulletin/pixel/2018-03-01	O-Goo-Andro/16-04-18/133
NA	16-03-2018	4.6	In Android for MSM, Firefox OS for MSM, QRD Android, with all Android releases from CAF using the Linux kernel, improper controls in MSM CORE leads to use memory after it is freed in msm_core_ioctl(). **CVE-ID:CVE-2017-18066**	href=https://source.codeaurora.org/quic/la/kernel/msm-3.18/commit/?id=ff11f44c0c10c94170f03a8698f73f7e08b74625,href=https://source.android.com/security/bulletin/pixel/2018-03-01	O-Goo-Andro/16-04-18/134

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/ Patch	NCIIPCID
NA	16-03-2018	4.6	In Android for MSM, Firefox OS for MSM, QRD Android, with all Android releases from CAF using the Linux kernel, improper input validation for vdev_map in wmtbttoffset_update_event_handler(), which is received from firmware, leads to potential buffer overwrite and out of bounds memory read. **CVE-ID:CVE-2017-18050**	href=https://source.codeaurora.org/quic/la/platform/vendor/qcom-opensource/wlan/qcacld-3.0/commit/?id=63b57442d65dfdb4b4634ff32059b1bca8c72fb7,href=https://source.android.com/security/bulletin/pixel/2018-03-01	O-Goo-Andro/16-04-18/135
NA	16-03-2018	4.6	In Android for MSM, Firefox OS for MSM, QRD Android, with all Android releases from CAF using the Linux kernel, there is an obsolete set/reset ssid hotlist API. **CVE-ID:CVE-2017-11074**	href=https://source.android.com/security/bulletin/pixel/2018-03-01,href=https://source.codeaurora.org/quic/la/platform/vendor/qcom-opensource/wlan/prima/commit/?id=f5ae7b35c90f14b7e66b3a91d4fb247563a8a22b	O-Goo-Andro/16-04-18/136
NA	16-03-2018	5	In Android for MSM, Firefox OS for MSM, QRD Android, with all Android releases from CAF using the Linux kernel, improper input validation for cmpl_params->num_reports, param_buf->desc_ids and param_buf->status in wmmgmt_tx_bundle_completion_handler(), which is received from firmware, leads to potential out of bounds memory read. **CVE-ID:CVE-2017-18052**	href=https://source.codeaurora.org/quic/la/platform/vendor/qcom-opensource/wlan/qcacld-3.0/commit/?id=c04c4870bd86a5f878553d7acf207388f3d6c3bd,href=https://source.android.com/security/bulletin/pixel/2018-03-01	O-Goo-Andro/16-04-18/137

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/ Patch	NCIIPCID
NA	16-03-2018	5	In Android for MSM, Firefox OS for MSM, QRD Android, with all Android releases from CAF using the Linux kernel, improper input validation for event->vdev_id in wmrcpi_event_handler(), which is received from firmware, leads to potential out of bounds memory read. **CVE-ID:CVE-2017-18051**	href=https://source.codeaurora.org/quic/la/platform/vendor/qcom-opensource/wlan/qcacld-3.0/commit/?id=38fba6a9f6ca3c7bf0c4c1bd84fa2b89fbcaeb93,href=https://source.android.com/security/bulletin/pixel/2018-03-01	O-Goo-Andro/16-04-18/138
NA	16-03-2018	5	In Android for MSM, Firefox OS for MSM, QRD Android, with all Android releases from CAF using the Linux kernel, improper input validation for fix_param->vdev_id in wmp2lo_event_handler(), which is received from firmware, leads to potential out of bounds memory read. **CVE-ID:CVE-2017-18053**	href=https://source.codeaurora.org/quic/la/platform/vendor/qcom-opensource/wlan/qcacld-3.0/commit/?id=da1c6e996ac7635c202296e31118f088f9427947,href=https://source.android.com/security/bulletin/pixel/2018-03-01	O-Goo-Andro/16-04-18/139
NA	16-03-2018	5	In Android for MSM, Firefox OS for MSM, QRD Android, with all Android releases from CAF using the Linux kernel, improper input validation for resevent->vdev_id in wmunified_bcntx_status_event_handler(), which is received from firmware, leads to potential out of bounds memory read. **CVE-ID:CVE-2017-18060**	href=https://source.codeaurora.org/quic/la/platform/vendor/qcom-opensource/wlan/qcacld-3.0/commit/?id=f3d81bd0b3cb992c214d94196b33168b02589c6b,href=https://source.android.com/security/bulletin/pixel/2018-03-01	O-Goo-Andro/16-04-18/140

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/ Patch	NCIIPCID
NA	16-03-2018	5	In Android for MSM, Firefox OS for MSM, QRD Android, with all Android releases from CAF using the Linux kernel, improper input validation for vdev id in wmnlo_scan_cmevt_handler(), which is received from firmware, leads to potential out of bounds memory read. **CVE-ID:CVE-2017-18057**	href=https://source.codeaurora.org/quic/la/platform/vendor/qcom-opensource/wlan/qcacld-3.0/commit/?id=24d41d2bd3d98325b3800345f4ba27a334b3894b,href=https://source.android.com/security/bulletin/pixel/2018-03-01	O-Goo-Andro/16-04-18/141
NA	16-03-2018	5	In Android for MSM, Firefox OS for MSM, QRD Android, with all Android releases from CAF using the Linux kernel, improper input validation for vdev id in wmscan_event_callback(), which is received from firmware, leads to potential out of bounds memory read. **CVE-ID:CVE-2017-18059**	href=https://source.codeaurora.org/quic/la/platform/vendor/qcom-opensource/wlan/qcacld-3.0/commit/?id=217705da7726002ffe61dad51a6c9cc97c52f649,href=https://source.android.com/security/bulletin/pixel/2018-03-01	O-Goo-Andro/16-04-18/142
NA	16-03-2018	5	In Android for MSM, Firefox OS for MSM, QRD Android, with all Android releases from CAF using the Linux kernel, improper input validation for wow_buf_pkt_len in wmwow_wakeuhost_event() which is received from firmware leads to potential out of bounds memory read. **CVE-ID:CVE-2017-18058**	href=https://source.codeaurora.org/quic/la/platform/vendor/qcom-opensource/wlan/qcacld-3.0/commit/?id=d6d42a10d4abf09299cdfacdd8aed5c26731b5ff,href=https://source.android.com/security/bulletin/pixel/2018-03-01	O-Goo-Andro/16-04-18/143

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/ Patch	NCIIPCID
Execute Code	16-03-2018	4.6	In Android for MSM, Firefox OS for MSM, QRD Android, with all Android releases from CAF using the Linux kernel, improper input validation for vent->vdev_id in wmaction_frame_filter_mac_event_handler(), which is received from firmware, leads to arbitrary code execution. **CVE-ID:CVE-2017-18065**	href=https://source.codeaurora.org/quic/la/platform/vendor/qcom-opensource/wlan/qcacld-3.0/commit/?id=a8bc0f90ef49ea0aee90047a17772e4eebff259a,href=https://source.android.com/security/bulletin/pixel/2018-03-01	O-Goo-Andro/16-04-18/144
Gain Informatyion	16-03-2018	4.6	In Android for MSM, Firefox OS for MSM, QRD Android, with all Android releases from CAF using the Linux kernel, untrusted pointer dereference in update_userspace_power() function in power leads to information exposure. **CVE-ID:CVE-2017-15833**	href=https://source.codeaurora.org/quic/la/kernel/msm-3.10/commit/?id=51ce6aec73d80e1f1fcc9c7fa71e9c2fcbdbc0fd,href=https://source.android.com/security/bulletin/pixel/2018-03-01	O-Goo-Andro/16-04-18/145
Overflow	16-03-2018	4.4	In Android for MSM, Firefox OS for MSM, QRD Android, with all Android releases from CAF using the Linux kernel, due to a race condition in a firmware loading routine, a buffer overflow could potentially occur if multiple user space threads try to update the WLAN firmware file through sysfs. **CVE-ID:CVE-2017-11082**	href=https://source.android.com/security/bulletin/pixel/2018-03-01,href=https://source.codeaurora.org/quic/la//kernel/msm-3.10/commit/?id=2d4f8cd8d11f8fb1491a20d7e316cc0fd03eeb59	O-Goo-Andro/16-04-18/146

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/ Patch	NCIIPCID
Overflow	16-03-2018	4.4	In Android for MSM, Firefox OS for MSM, QRD Android, with all Android releases from CAF using the Linux kernel, race condition in diag_dbgfs_read_dcistats(), while accessing diag_dbgfs_dci_datindex, causes potential heap overflow. **CVE-ID:CVE-2017-15834**	href=https://source.codeaurora.org/quic/la/kernel/msm-3.18/commit/?id=2e1b54e38f1516e70d9f6581c4f1ee935effb903,href=https://source.android.com/security/bulletin/pixel/2018-03-01	O-Goo-Andro/16-04-18/147
Overflow	16-03-2018	4.6	In Android for MSM, Firefox OS for MSM, QRD Android, with all Android releases from CAF using the Linux kernel, improper ch_list array index initialization in function sme_set_plm_request() causes potential buffer overflow. **CVE-ID:CVE-2017-15830**	href=https://source.codeaurora.org/quic/la/platform/vendor/qcom-opensource/wlan/qcacld-3.0/commit/?id=8a7a2a9c5d203e3395811963061c79d3bc257ebe,href=https://source.android.com/security/bulletin/pixel/2018-03-01	O-Goo-Andro/16-04-18/148
Overflow	16-03-2018	4.6	In Android for MSM, Firefox OS for MSM, QRD Android, with all Android releases from CAF using the Linux kernel, improper input validation for num_vdev_mac_entries in wmpdev_hw_mode_transition_evt_handler(), which is received from firmware, leads to potential buffer overflow. **CVE-ID:CVE-2017-18054**	href=https://source.codeaurora.org/quic/la/platform/vendor/qcom-opensource/wlan/qcacld-3.0/commit/?id=6eefc756612e39fab49ff719b3dc9b94def53396,href=https://source.android.com/security/bulletin/pixel/2018-03-01	O-Goo-Andro/16-04-18/149

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/ Patch	NCIIPCID
Overflow	16-03-2018	4.6	In Android for MSM, Firefox OS for MSM, QRD Android, with all Android releases from CAF using the Linux kernel, improper input validation for wmi_event->num_vdev_mac_entries in wmpdev_set_hw_mode_resevt_handler(), which is received from firmware, leads to potential buffer overflow. **CVE-ID:CVE-2017-18055**	href=https://source.codeaurora.org/quic/la/platform/vendor/qcom-opensource/wlan/qcacld-3.0/commit/?id=50a0554d12cff58b3ffbd51d3194304244b87023,href=https://source.android.com/security/bulletin/pixel/2018-03-01	O-Goo-Andro/16-04-18/150
Overflow	16-03-2018	4.6	In Android for MSM, Firefox OS for MSM, QRD Android, with all Android releases from CAF using the Linux kernel, in the function wmndend_indication_event_handler(), there is no input validation check on a event_info value coming from firmware, which can cause an integer overflow and then leads to potential heap overwrite. **CVE-ID:CVE-2017-15831**	href=https://source.codeaurora.org/quic/la/platform/vendor/qcom-opensource/wlan/qcacld-3.0/commit/?id=31e6a657320e4299c659e3d57d38a89afe8c1ce1,href=https://source.android.com/security/bulletin/pixel/2018-03-01	O-Goo-Andro/16-04-18/151
Overflow	16-03-2018	4.6	In Android for MSM, Firefox OS for MSM, QRD Android, with all Android releases from CAF using the Linux kernel, in the processing of messages of type eWNI_SME_MODIFY_ADDITIONAL_IES, an integer overflow leading to heap buffer overflow may potentially occur. **CVE-ID:CVE-2017-14887**	href=https://source.codeaurora.org/quic/la/platform/vendor/qcom-opensource/wlan/qcacld-3.0/commit/?id=4ce28e7c85f89e2c3555ec840b6adda47bd5dab0,href=https://source.android.com/security/bulletin/pixel/2018-03-01	O-Goo-Andro/16-04-18/152

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/ Patch	NCIIPCID
Overflow	16-03-2018	4.6	In Android for MSM, Firefox OS for MSM, QRD Android, with all Android releases from CAF using the Linux kernel, potential buffer overflow can happen when processing AOA measurement event from WIGIG firmware in wil_aoevt_meas(). **CVE-ID:CVE-2017-18061**	href=https://source.codeaurora.org/quic/la/kernel/msm-3.18/commit/?id=b65cf2a007e88fe86dbd6d3269682fc585a4130f,href=https://source.android.com/security/bulletin/pixel/2018-03-01	O-Goo-Andro/16-04-18/153
Overflow	16-03-2018	4.6	In Android for MSM, Firefox OS for MSM, QRD Android, with all Android releases from CAF using the Linux kernel, potential buffer overflow can happen when processing UTF event in wmprocess_utf_event(). **CVE-ID:CVE-2017-18062**	href=https://source.codeaurora.org/quic/la/platform/vendor/qcom-opensource/wlan/qcacld-3.0/commit/?id=d7927eb7c9c2d79a3e24cddd1e9447ab98bf6700,href=https://source.android.com/security/bulletin/pixel/2018-03-01	O-Goo-Andro/16-04-18/154
Huawei					
Fusionsphere Openstack Firmware					
NA	20-03-2018	6.5	Huawei FusionSphere OpenStack V100R006C00SPC102(NFV) has a privilege escalation vulnerability. Due to improper privilege restrictions, an attacker with high privilege may obtain the other users' certificates. Successful exploit may cause privilege escalation. **CVE-ID:CVE-2017-8187**	NA	O-Hua-Fusio/16-04-18/155

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/ Patch	NCIIPCID
Mate 9 Pro Firmware					
Execute Code	20-03-2018	9.3	Huawei Mate 9 Pro smartphones with software of LON-AL00BC00B139D, LON-AL00BC00B229, LON-L29DC721B188 have a memory double free vulnerability. The system does not manage the memory properly, that frees on the same memory address twice. An attacker tricks the user who has root privilege to install a crafted application, successful exploit could result in malicious code execution. **CVE-ID:CVE-2017-17320**		O-Hua-Mate/16-04-18/156
Linux					
Linux Kernel					
NA	16-03-2018	7.2	A flaw was found in the Linux 4.x kernel's implementation of 32-bit syscall interface for bridging. This allowed a privileged user to arbitrarily write to a limited range of kernel memory. **CVE-ID:CVE-2018-1068**	href=https://bugzilla.redhat.com/show_bug.cgi?id=1552048,href=https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=b71812168571fa55e44cdd0254471331b9c4c4c6,href=https://github.com/torvalds/linux/commit/b71812168571fa55e44cdd0254471331b9c4c4c6,href=https://marc.info/?l=linux-netdev&m=152023808817590&w=2,href=https://marc.info/?l=linux-netdev&m=152025888924151&w=2	O-Lin-Linux-16-04-18/157

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

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