National Critical Information Infrastructure Protection Centre

CVE Report

CV Scoring Scale : 3-10 **16-30 Nov 2017** **Vol. 04 No.20**

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Application					
Altran					
Picotcp					
DoS Execute Code Overflow	16-11-2017	7.5	picoTCP (versions 1.7.0 - 1.5.0) is vulnerable to stack buffer overflow resulting in code execution or denial of service attack **CVE ID : CVE 2017-1000210**	https://github.com/tass-belgium/picotcp/pull/473	A-ALT-PICOT-11217/1
Cisco					
Registered Envelope Service					
Execute Code XSS	16-11-2017	4.3	Multiple vulnerabilities in the web interface of the Cisco Registered Envelope Service (a cloud-based service) could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack or redirect a user of the affected service to an undesired web page. The vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface of the affected service. An attacker could exploit these vulnerabilities by persuading a user to click a malicious link or by sending an HTTP request that could cause the affected service to redirect the request to a specified malicious URL. A successful exploit could allow the attacker to execute arbitrary script code in the context of the web interface of the affected system or allow the attacker to access sensitive browser-based information on the affected system. These types of exploits could also be used in	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171115-res	A-CIS-REGIS-11217/2

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			phishing attacks that send users to malicious websites without their knowledge. Cisco Bug IDs: CSCve77195, CSCve90978, CSCvf42310, CSCvf42703, CSCvf42723, CSCvf46169, CSCvf49999. **CVE ID : CVE 2017-12323**		
Execute Code XSS	16-11-2017	4.3	Multiple vulnerabilities in the web interface of the Cisco Registered Envelope Service (a cloud-based service) could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack or redirect a user of the affected service to an undesired web page. The vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface of the affected service. An attacker could exploit these vulnerabilities by persuading a user to click a malicious link or by sending an HTTP request that could cause the affected service to redirect the request to a specified malicious URL. A successful exploit could allow the attacker to execute arbitrary script code in the context of the web interface of the affected system or allow the attacker to access sensitive browser-based information on the affected system. These types of exploits could also be used in phishing attacks that send users to malicious websites without their knowledge. Cisco Bug IDs: CSCve77195, CSCve90978, CSCvf42310, CSCvf42703, CSCvf42723, CSCvf46169, CSCvf49999. **CVE ID : CVE 2017-12321**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171115-res	A-CIS-REGIS-11217/3
Execute Code	16-11-2017	4.3	Multiple vulnerabilities in the web	https://tools.cis	A-CIS-

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
XSS			interface of the Cisco Registered Envelope Service (a cloud-based service) could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack or redirect a user of the affected service to an undesired web page. The vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface of the affected service. An attacker could exploit these vulnerabilities by persuading a user to click a malicious link or by sending an HTTP request that could cause the affected service to redirect the request to a specified malicious URL. A successful exploit could allow the attacker to execute arbitrary script code in the context of the web interface of the affected system or allow the attacker to access sensitive browser-based information on the affected system. These types of exploits could also be used in phishing attacks that send users to malicious websites without their knowledge. Cisco Bug IDs: CSCve77195, CSCve90978, CSCvf42310, CSCvf42703, CSCvf42723, CSCvf46169, CSCvf49999. **CVE ID : CVE 2017-12320**	co.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171115-res	REGIS-11217/4
Cisco/Cisco					
Emergency Responder;Finesse;Hosted Collaboration Solution;Mediasense;Prime License Manager;Socialminer;Unified Communications Manager;Unified Communications Manager Im And Presence Service;Unified Contact Center Express;Unity Connection/Unified Intelligence Center					
NA	16-11-2017	10	A vulnerability in the upgrade mechanism of Cisco collaboration products based on the Cisco Voice Operating System software platform could allow an unauthenticated, remote attacker to gain	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171115-	A-CIS-EMERG-11217/5

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	Patch	NCIIPC ID
			unauthorized, elevated access to an affected device. The vulnerability occurs when a refresh upgrade (RU) or Prime Collaboration Deployment (PCD) migration is performed on an affected device. When a refresh upgrade or PCD migration is completed successfully, an engineering flag remains enabled and could allow root access to the device with a known password. If the vulnerable device is subsequently upgraded using the standard upgrade method to an Engineering Special Release, service update, or a new major release of the affected product, this vulnerability is remediated by that action. Note: Engineering Special Releases that are installed as COP files, as opposed to the standard upgrade method, do not remediate this vulnerability. An attacker who can access an affected device over SFTP while it is in a vulnerable state could gain root access to the device. This access could allow the attacker to compromise the affected system completely. Cisco Bug IDs: CSCvg22923, CSCvg55112, CSCvg55128, CSCvg55145, CSCvg58619, CSCvg64453, CSCvg64456, CSCvg64464, CSCvg64475, CSCvg68797. **CVE ID : CVE 2017-12337**	vos	
Creolabs					
Gravity					
Execute Code Overflow	16-11-2017	7.5	Creolabs Gravity Version: 1.0 Heap Overflow Potential Code Execution. By creating a large loop whiling pushing data to a buffer, we can break out of the bounds checking of that buffer. When list.join is called on	https://github.com/marcobambini/gravity/issues/172	A-CRE-GRAVI-11217/6

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	Patch	NCIIPC ID
			the data it will read past a buffer resulting in a Heap-Buffer-Overflow. **CVE ID : CVE 2017-1000173**		
Execute Code	16-11-2017	7.5	Creolabs Gravity Version: 1.0 Use-After-Free Possible code execution. An example of a Heap-Use-After-Free after the 'sublexer' pointer has been freed. Line 542 of gravity_lexer.c. 'lexer' is being used to access a variable but 'lexer' has already been freed, creating a Heap Use-After-Free condition. **CVE ID : CVE 2017-1000172**	https://github.com/marcobambini/gravity/issues/144	A-CRE-GRAVI-11217/7
Exiv2					
Exiv2					
NA	17-11-2017	4.3	Exiv2 0.26 contains a stack out of bounds read in JPEG2000 parser **CVE ID : CVE 2017-1000128**	http://www.openwall.com/lists/oss-security/2017/06/30/1	A-EXI-EXIV2-11217/8
Overflow	17-11-2017	4.3	Exiv2 0.26 contains a heap buffer overflow in tiff parser **CVE ID : CVE 2017-1000127**	http://www.openwall.com/lists/oss-security/2017/06/30/1	A-EXI-EXIV2-11217/9
NA	17-11-2017	4.3	exiv2 0.26 contains a Stack out of bounds read in webp parser **CVE ID : CVE 2017-1000126**	http://www.openwall.com/lists/oss-security/2017/06/30/1	A-EXI-EXIV2-11217/10
I Librarian					
I Librarian					
XSS	16-11-2017	4.3	I, Librarian version <=4.6 & 4.7 is vulnerable to Reflected Cross-Site Scripting in the temp.php resulting in an attacker being able to inject malicious client side scripting which will be executed in the browser of users if they visit the manipulated site. **CVE ID : CVE 2017-1000236**	https://www.sec-consult.com/fxdata/seccons/prod/temedia/advisories_txt/20170509-0_I_Librarian_Multiple_vulnerabilities_v10.txt	A-I-L-I LIB-11217/11
Gain	16-11-2017	5	I, Librarian version <=4.6 & 4.7 is	https://www.se	A-I-L-I

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	Patch	NCIIPC ID
Information			vulnerable to Directory Enumeration in the jqueryFileTree.php resulting in attacker enumerating directories simply by navigating through the "dir" parameter **CVE ID : CVE 2017-1000234**	c-consult.com/fxdata/seccons/prod/temedia/advisories_txt/20170509-0_I_Librarian_Multiple_vulnerabilities_v10.txt	LIB-11217/12
NA	16-11-2017	7.5	I, Librarian version <=4.6 & 4.7 is vulnerable to Server-Side Request Forgery in the ajaxsupplement.php resulting in the attacker being able to reset any user's password. **CVE ID : CVE 2017-1000237**	https://www.sec-consult.com/fxdata/seccons/prod/temedia/advisories_txt/20170509-0_I_Librarian_Multiple_vulnerabilities_v10.txt	A-I-L-I LIB-11217/13
NA	16-11-2017	10	I, Librarian version <=4.6 & 4.7 is vulnerable to OS Command Injection in batchimport.php resulting the web server being fully compromised. **CVE ID : CVE 2017-1000235**	https://www.sec-consult.com/fxdata/seccons/prod/temedia/advisories_txt/20170509-0_I_Librarian_Multiple_vulnerabilities_v10.txt	A-I-L-I LIB-11217/14
Invoiceplane					
Invoiceplane					
XSS	16-11-2017	3.5	InvoicePlane version 1.4.10 is vulnerable to a Stored Cross Site Scripting resulting in allowing an authenticated user to inject malicious client side script which will be executed in the browser of users if they visit the manipulated site. **CVE ID : CVE 2017-1000239**	https://www.sec-consult.com/fxdata/seccons/prod/temedia/advisories_txt/20170523-0_InvoicePlane_Upload_arbitrary_files_stored_XSS_v10.txt	A-INV-INVOI-11217/15
NA	16-11-2017	6.5	InvoicePlane version 1.4.10 is	https://www.se	A-INV-

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	Patch	NCIIPC ID
			vulnerable to a Arbitrary File Upload resulting in an authenticated user can upload a malicious file to the webserver. It is possible for an attacker to upload a script which is able to compromise the webserver. **CVE ID : CVE 2017-1000238**	c-consult.com/fxdata/seccons/prod/temedia/advisories_txt/20170523-0_InvoicePlane_Upload_arbitrary_files_stored_XSS_v10.txt	INVOI-11217/16
Lightftp Project					
Lightftp					
DoS Execute Code Overflow	16-11-2017	7.5	LightFTP version 1.1 is vulnerable to a buffer overflow in the "writelogentry" function resulting a denial of services or a remote code execution. **CVE ID : CVE 2017-1000218**	https://github.com/hfiref0x/LightFTP/issues/5	A-LIG-LIGHT-11217/17
Nlnetlabs					
Ldns					
NA	16-11-2017	7.5	A double-free vulnerability in str2host.c in ldns 1.7.0 have unspecified impact and attack vectors. **CVE ID : CVE 2017-1000232**	https://www.nlnetlabs.nl/bugs-script/show_bug.cgi?id=1257	A-NLN-LDNS-11217/18
NA	16-11-2017	7.5	A double-free vulnerability in parse.c in ldns 1.7.0 have unspecified impact and attack vectors. **CVE ID : CVE 2017-1000231**	https://www.nlnetlabs.nl/bugs-script/show_bug.cgi?id=1256	A-NLN-LDNS-11217/19
Octobercms					
October Cms					
Execute Code XSS	16-11-2017	4.3	October CMS build 412 is vulnerable to stored WCI (a.k.a XSS) in brand logo image name resulting in JavaScript code execution in the victim's browser. **CVE ID : CVE 2017-1000193**	https://github.com/octobercms/october/compare/v1.0.412...v1.0.413#diff-66d6dfe5e11488e1afefcb69b8bdaabfR31	A-OCT-OCTOB-11217/20
NA	16-11-2017	6.4	October CMS build 412 is vulnerable to PHP object injection in asset move	https://github.com/octobercms	A-OCT-OCTOB-

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	Patch	NCIIPC ID
			functionality resulting in ability to delete files limited by file permissions on the server. **CVE ID : CVE 2017-1000195**	/october/compare/v1.0.412...v1.0.413#diff-c328b7b99eac0d17b3c71eb37038fd61R317	11217/21
NA	16-11-2017	7.5	October CMS build 412 is vulnerable to file path modification in asset move functionality resulting in creating creating malicious files on the server. **CVE ID : CVE 2017-1000197**	https://github.com/octobercms/october/compare/v1.0.412...v1.0.413#diff-eef90a4e3585febf6489916dc242d0ceR241	A-OCT-OCTOB-11217/22
Exec Code	16-11-2017	7.5	October CMS build 412 is vulnerable to PHP code execution in the asset manager functionality resulting in site compromise and possibly other applications on the server. **CVE ID : CVE 2017-1000196**	https://github.com/octobercms/october/compare/v1.0.412...v1.0.413#diff-c328b7b99eac0d17b3c71eb37038fd61R49	A-OCT-OCTOB-11217/23
NA	16-11-2017	7.5	October CMS build 412 is vulnerable to Apache configuration modification via file upload functionality resulting in site compromise and possibly other applications on the server. **CVE ID : CVE 2017-1000194**	https://github.com/octobercms/october/compare/v1.0.412...v1.0.413#diff-c328b7b99eac0d17b3c71eb37038fd61R224	A-OCT-OCTOB-11217/24
Open-emr					
Openemr					
XSS	16-11-2017	3.5	The application OpenEMR is affected by multiple reflected & stored Cross-Site Scripting (XSS) vulnerabilities affecting version 5.0.0 and prior versions. These vulnerabilities could allow remote authenticated attackers to inject arbitrary web script or HTML. **CVE ID : CVE 2017-1000240**	https://www.wizlynxgroup.com/security-research-advisories/vuln/WLX-2017-001	A-OPE-OPENE-11217/25
NA	16-11-2017	6.5	The application OpenEMR version 5.0.0, 5.0.1-dev and prior is affected	https://www.wizlynxgroup.co	A-OPE-OPENE-

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	Patch	NCIIPC ID
			by vertical privilege escalation vulnerability. This vulnerability can allow an authenticated non-administrator users to view and modify information only accessible to administrators. **CVE ID : CVE 2017-1000241**	m/security-research-advisories/vuln/WLX-2017-004	11217/26
Pidusage Project					
Pidusage					
Execute Code	16-11-2017	7.5	soyuka/pidusage <=1.1.4 is vulnerable to command injection in the module resulting in arbitrary command execution **CVE ID : CVE 2017-1000220**	https://nodesecurity.io/advisories/356	A-PID-PIDUS-11217/27
S9Y					
Serendipity					
Sql	17-11-2017	5	Serendipity 2.0.3 is vulnerable to a SQL injection in the blog component resulting in information disclosure **CVE ID : CVE 2017-1000129**	https://blog.s9y.org/archives/269-Serendipity-2.0.4-and-2.1-beta2-released.html	A-S9Y-SEREN-11217/28
Swftools					
Swftools					
Overflow	16-11-2017	4.3	In SWFTools, an address access exception was found in pdf2swf. FoFiTrueType::writeTTF() **CVE ID : CVE 2017-1000187**	https://github.com/matthiaskramm/swftools/issues/36	A-SWF-SWFTO-11217/29
Overflow	16-11-2017	4.3	In SWFTools, a stack overflow was found in pdf2swf. **CVE ID : CVE 2017-1000186**	https://github.com/matthiaskramm/swftools/issues/34	A-SWF-SWFTO-11217/30
Overflow	16-11-2017	4.3	In SWFTools, a memcpy buffer overflow was found in gif2swf. **CVE ID : CVE 2017-1000185**	https://github.com/matthiaskramm/swftools/issues/33	A-SWF-SWFTO-11217/31
Overflow	16-11-2017	4.3	In SWFTools, a memory leak was found in wav2swf. **CVE ID : CVE 2017-1000182**	https://github.com/matthiaskramm/swftools/issues/30	A-SWF-SWFTO-11217/32
Overflow	16-11-2017	4.3	In SWFTools, a memcpy buffer	https://github.c	A-SWF-

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			overflow was found in swfc. **CVE ID : CVE 2017-1000176**	om/matthiaskramm/swftools/issues/23	SWFTO-11217/33
Overflow	16-11-2017	4.3	In SWFTools, an address access exception was found in swfdump swf_GetBits(). **CVE ID : CVE 2017-1000174**	https://github.com/matthiaskramm/swftools/issues/21	A-SWF-SWFTO-11217/34
DoS Overflow	17-11-2017	4.3	In SWFTools 0.9.2, the wav_convert2mono function in lib/wav.c does not properly restrict a multiplication within a malloc call, which allows remote attackers to cause a denial of service (integer overflow and NULL pointer dereference) via a crafted WAV file. **CVE ID : CVE 2017-16868**	https://github.com/matthiaskramm/swftools/issues/52	A-SWF-SWFTO-11217/35
Tcmu-runner Project					
Tcmu-runner					
DoS	16-11-2017	5	tcmu-runner version 1.0.5 to 1.2.0 is vulnerable to a dbus triggered NULL pointer dereference in the tcmu-runner daemon's on_unregister_handler() function resulting in denial of service **CVE ID : CVE 2017-1000200**	https://github.com/open-iscsi/tcmu-runner/pull/200/commits/bb80e9c7a798f035768260ebdadffb6eb0786178	A-TCM-TCMU--11217/36
Gain Information	16-11-2017	5	tcmu-runner version 0.91 up to 1.20 is vulnerable to information disclosure in handler_qcow.so resulting in non-privileged users being able to check for existence of any file with root privileges. **CVE ID : CVE 2017-1000199**	https://github.com/open-iscsi/tcmu-runner/issues/194	A-TCM-TCMU--11217/37
DoS Overflow	16-11-2017	5	tcmu-runner daemon version 0.9.0 to 1.2.0 is vulnerable to invalid memory references in the handler_glfs.so handler resulting in denial of service **CVE ID : CVE 2017-1000198**	https://github.com/open-iscsi/tcmu-runner/commit/61bd03e600d2abf309173e9186f4d465bb1b7157	A-TCM-TCMU--11217/38
Tine20					
Tine 2.0					

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	Patch	NCIIPC ID
Execute Code XSS	17-11-2017	3.5	Tine 2.0 version 2017.02.4 is vulnerable to XSS in the Addressbook resulting code execution and privilege escalation **CVE ID : CVE 2017-1000164**	https://forge.tine20.org/view.php?id=13228	A-TIN-TINE -11217/39
Wbce					
Wbce Cms					
XSS	16-11-2017	3.5	WBCE v1.1.11 is vulnerable to reflected XSS via the "begriff" POST parameter in /admin/admintools/tool.php?tool=user_search **CVE ID : CVE 2017-1000213**	https://github.com/WBCE/WBCE_CMS/commit/0da620016aec17ac2d2f3a22c55ab8c2b55e691e#diff-7b380285e285160d0070863099baabe0	A-WBC-WBCE -11217/40
Zohocorp					
Manageengine Applications Manager					
Sql	16-11-2017	7.5	Zoho ManageEngine Applications Manager 13 allows SQL injection via the /MyPage.do widgetid parameter. **CVE ID : CVE 2017-16851**	http://code610.blogspot.com/2017/11/more-sql-injections-in-manageengine.html	A-ZOH-MANAG-11217/41
Sql	16-11-2017	7.5	Zoho ManageEngine Applications Manager 13 allows SQL injection via the /showresource.do resourceid parameter in a getResourceProfiles action. **CVE ID : CVE 2017-16850**	http://code610.blogspot.com/2017/11/more-sql-injections-in-manageengine.html	A-ZOH-MANAG-11217/42
Sql	16-11-2017	7.5	Zoho ManageEngine Applications Manager 13 allows SQL injection via the /MyPage.do?method=viewDashBoard forpage parameter. **CVE ID : CVE 2017-16849**	http://code610.blogspot.com/2017/11/more-sql-injections-in-manageengine.html	A-ZOH-MANAG-11217/43
Sql	16-11-2017	7.5	Zoho ManageEngine Applications Manager 13 allows SQL injection via the /manageConfMons.do	http://code610.blogspot.com/2017/11/more-	A-ZOH-MANAG-11217/44

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	Patch	NCIIPC ID
			groupname parameter. **CVE ID : CVE 2017-16848**	sql-injections-in-manageengine.html	
Sql	16-11-2017	7.5	Zoho ManageEngine Applications Manager 13 allows SQL injection via the /showresource.do resourceid parameter in a showPlasmaView action. **CVE ID : CVE 2017-16847**	http://code610.blogspot.com/2017/11/more-sql-injections-in-manageengine.html	A-ZOH-MANAG-11217/45
Sql	16-11-2017	7.5	Zoho ManageEngine Applications Manager 13 allows SQL injection via the /manageApplications.do?method=AddSubGroup haid parameter. **CVE ID : CVE 2017-16846**	http://code610.blogspot.com/2017/11/more-sql-injections-in-manageengine.html	A-ZOH-MANAG-11217/46
OPERATING SYSTEM(OS)					
Cisco					
Rf Gateway 1 Firmware					
DoS	16-11-2017	5	A vulnerability in the TCP state machine of Cisco RF Gateway 1 devices could allow an unauthenticated, remote attacker to prevent an affected device from delivering switched digital video (SDV) or video on demand (VoD) streams, resulting in a denial of service (DoS) condition. The vulnerability is due to a processing error with TCP connections to the affected device. An attacker could exploit this vulnerability by establishing a large number of TCP connections to an affected device and not actively closing those TCP connections. A successful exploit could allow the attacker to prevent the affected device from delivering SDV or VoD streams to set-top boxes. Cisco Bug IDs: CSCvf19887. **CVE ID : CVE 2017-12318**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171115-rf-gateway-1	O-CIS-RF GA-11217/47

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	Patch	NCIIPC ID
NA	16-11-2017	7.2	A vulnerability in Cisco Umbrella Insights Virtual Appliances 2.1.0 and earlier could allow an authenticated, local attacker to log in to an affected virtual appliance with root privileges. The vulnerability is due to the presence of default, static user credentials for an affected virtual appliance. An attacker could exploit this vulnerability by using the hypervisor console to connect locally to an affected system and then using the static credentials to log in to an affected virtual appliance. A successful exploit could allow the attacker to log in to the affected appliance with root privileges. Cisco Bug IDs: CSCvg31220. **CVE ID : CVE 2017-12350**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171115-uva	O-CIS-UMBRE-11217/48
Google					
Android					
Memory corruption	16-11-2017	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 the function audio_effects_shared_ioctl(), memory corruption can occur. **CVE ID : CVE 2017-11025**	https://source.android.com/security/bulletin/pixel/2017-11-01	O-GOO-ANDRO-11217/49
NA	16-11-2017	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 mdss_rotator_ioctl in the driver /dev/mdss_rotator, a Use-After-Free condition can potentially occur due to a fence being installed too early. **CVE ID : CVE 2017-11091**	https://source.android.com/security/bulletin/pixel/2017-11-01	O-GOO-ANDRO-11217/50
Overflow	16-11-2017	4.6	In android for MSM, Firefox OS for MSM, QRD Android, with all Android releases from CAF using the Linux kernel, an integer overflow leading to a buffer overflow due to improper bound checking in	https://source.android.com/security/bulletin/pixel/2017-11-01	O-GOO-ANDRO-11217/51

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			msm_audio_effects_virtualizer_handler, file msm-audio-effects-q6-v2.c **CVE ID : CVE 2017-11085**		
NA	16-11-2017	4.6	In android for MSM, Firefox OS for MSM, QRD Android, with all Android releases from CAF using the Linux kernel, the qcacld pktlog allows mapping memory via /proc/ath_pktlog/cld to user space. **CVE ID : CVE 2017-11073**	https://source.android.com/security/bulletin/pixel/2017-11-01	O-GOO-ANDRO-11217/52
Bypass	16-11-2017	4.6	In android for MSM, Firefox OS for MSM, QRD Android, with all Android releases from CAF using the Linux kernel, while processing the boot image header, range checks can be bypassed by supplying different versions of the header at the time of check and use. **CVE ID : CVE 2017-11038**	https://source.android.com/security/bulletin/pixel/2017-11-01	O-GOO-ANDRO-11217/53
Overflow Obtain Information	16-11-2017	4.6	In android for MSM, Firefox OS for MSM, QRD Android, with all Android releases from CAF using the Linux kernel, possible buffer overflow or information leak in the functions "sme_set_ft_ies" and "csr_roam_issue_ft_preauth_req" due to incorrect initialization of WEXT callbacks and lack of the checks for buffer size. **CVE ID : CVE 2017-11035**	https://source.android.com/security/bulletin/pixel/2017-11-01	O-GOO-ANDRO-11217/54
NA	16-11-2017	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 can occur when kmalloc fails to allocate memory for pointers resp/req in the service-locator driver function service_locator_send_msg(). **CVE ID : CVE 2017-11032**	https://source.android.com/security/bulletin/pixel/2017-11-01	O-GOO-ANDRO-11217/55
Overflow	16-11-2017	4.6	In android for MSM, Firefox OS for MSM, QRD Android, with all Android releases from CAF using the Linux kernel, camera application triggers	https://source.android.com/security/bulletin/pixel/2017-11-	O-GOO-ANDRO-11217/56

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			"user-memory-access" issue as the Camera CPP module Linux driver directly accesses the application provided buffer, which resides in user space. An unchecked userspace value (ioctl_ptr->len) is used to copy contents to a kernel buffer which can lead to kernel buffer overflow. **CVE ID : CVE 2017-11029**	01	
NA	16-11-2017	4.6	In android for MSM, Firefox OS for MSM, QRD Android, with all Android releases from CAF using the Linux kernel, while flashing UBI image, size is not validated for being smaller than minimum header size causing unintialized data access vulnerability. **CVE ID : CVE 2017-11027**	https://source.android.com/security/bulletin/pixel/2017-11-01	O-GOO-ANDRO-11217/57
NA	16-11-2017	4.6	In android for MSM, Firefox OS for MSM, QRD Android, with all Android releases from CAF using the Linux kernel, while flashing FRP partition using reference FRP unlock, authentication method can be compromised for static keys. **CVE ID : CVE 2017-11026**	https://source.android.com/security/bulletin/pixel/2017-11-01	O-GOO-ANDRO-11217/58
NA	16-11-2017	4.6	In android for MSM, Firefox OS for MSM, QRD Android, with all Android releases from CAF using the Linux kernel, a race condition in the rmnet USB control driver can potentially lead to a Use After Free condition. **CVE ID : CVE 2017-11024**	https://source.android.com/security/bulletin/pixel/2017-11-01	O-GOO-ANDRO-11217/59
NA	16-11-2017	4.6	In android for MSM, Firefox OS for MSM, QRD Android, with all Android releases from CAF using the Linux kernel, there is a possibility of out-of-bound buffer accesses due to no synchronization in accessing global variables by multiple threads. **CVE ID : CVE 2017-11023**	https://source.android.com/security/bulletin/pixel/2017-11-01	O-GOO-ANDRO-11217/60
Overflow	16-11-2017	4.6	In android for MSM, Firefox OS for MSM, QRD Android, with all Android	https://source.android.com/se	O-GOO-ANDRO-

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	Patch	NCIIPC ID
			releases from CAF using the Linux kernel, array access out of bounds may occur in the camera driver in the kernel **CVE ID : CVE 2017-11018**	curity/bulletin/pixel/2017-11-01	11217/61
Overflow	16-11-2017	4.6	In android for MSM, Firefox OS for MSM, QRD Android, with all Android releases from CAF using the Linux kernel, while flashing a specially crafted UBI image, it is possible to corrupt memory, or access uninitialized memory. **CVE ID : CVE 2017-11017**	https://source.android.com/security/bulletin/2017-11-01	O-GOO-ANDRO-11217/62
Overflow	16-11-2017	4.6	In android for MSM, Firefox OS for MSM, QRD Android, with all Android releases from CAF using the Linux kernel, when processing a specially crafted QCA_NL80211_VENDOR_SUBCMD_ENCRYPTION_TEST cfg80211 vendor command a stack-based buffer overflow can occur. **CVE ID : CVE 2017-11012**	https://source.android.com/security/bulletin/pixel/2017-11-01	O-GOO-ANDRO-11217/63
Overflow	16-11-2017	4.6	In android for MSM, Firefox OS for MSM, QRD Android, with all Android releases from CAF using the Linux kernel, in the boot loader, a buffer overflow can occur while parsing the splash image. **CVE ID : CVE 2017-9721**	https://source.android.com/security/bulletin/pixel/2017-11-01	O-GOO-ANDRO-11217/64
Gain Information	16-11-2017	5	In android for MSM, Firefox OS for MSM, QRD Android, with all Android releases from CAF using the Linux kernel, buffer Over-read in Display due to the lack of an upper-bound validation when reading "num_of_cea_blocks" from the untrusted source (EDID), kernel memory can be exposed. **CVE ID : CVE 2017-11093**	https://source.android.com/security/bulletin/pixel/2017-11-01	O-GOO-ANDRO-11217/65
Gain Information	16-11-2017	5	In android for MSM, Firefox OS for MSM, QRD Android, with all Android releases from CAF using the Linux	https://source.android.com/security/bulletin/	O-GOO-ANDRO-11217/66

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			kernel, a buffer overread is observed in __wlan_hdd_cfg80211_set_pmksa when user space application sends PMKID of size less than WLAN_PMKID_LEN bytes. **CVE ID : CVE 2017-11090**	pixel/2017-11-01	
Gain Information	16-11-2017	5	In android for MSM, Firefox OS for MSM, QRD Android, with all Android releases from CAF using the Linux kernel, a buffer overread is observed in nl80211_set_station when user space application sends attribute NL80211_ATTR_LOCAL_MESH_POWER_MODE with data of size less than 4 bytes **CVE ID : CVE 2017-11089**	https://source.android.com/security/bulletin/pixel/2017-11-01	O-GOO-ANDRO-11217/67
NA	16-11-2017	5	In android for MSM, Firefox OS for MSM, QRD Android, with all Android releases from CAF using the Linux kernel, while processing a specially crafted cfg80211 vendor command, a buffer over-read can occur. **CVE ID : CVE 2017-11058**	https://source.android.com/security/bulletin/pixel/2017-11-01	O-GOO-ANDRO-11217/68
Gain Information	16-11-2017	5	In android for MSM, Firefox OS for MSM, QRD Android, with all Android releases from CAF using the Linux kernel, in the ISP Camera driver, the contents of an arbitrary kernel address can be leaked to userspace by the function msm_isp_get_stream_common_data() . **CVE ID : CVE 2017-11028**	https://source.android.com/security/bulletin/2017-11-01	O-GOO-ANDRO-11217/69
Gain Information	16-11-2017	5	In android for MSM, Firefox OS for MSM, QRD Android, with all Android releases from CAF using the Linux kernel, the probe requests originated from user's phone contains the information elements which specifies the supported wifi features. This shall impact the user's privacy if someone sniffs the probe requests originated by this DUT. Hence,	https://source.android.com/security/bulletin/pixel/2017-11-01	O-GOO-ANDRO-11217/70

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	Patch	NCIIPC ID
			control the presence of information elements using ini file. **CVE ID : CVE 2017-11022**		
Gain Information	16-11-2017	5	In android for MSM, Firefox OS for MSM, QRD Android, with all Android releases from CAF using the Linux kernel, missing race condition protection while updating msg mask table can lead to buffer over-read. Also access to freed memory can happen while updating msg_mask information. **CVE ID : CVE 2017-8279**	https://source.android.com/security/bulletin/pixel/2017-11-01	O-GOO-ANDRO-11217/71
DoS	16-11-2017	5	A denial of service vulnerability in the Android framework (syncstorageengine). Product: Android. Versions: 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2. Android ID: A-35028827. **CVE ID : CVE 2017-0845**	https://source.android.com/security/bulletin/pixel/2017-11-01	O-GOO-ANDRO-11217/72
Overflow	16-11-2017	7.2	In android for MSM, Firefox OS for MSM, QRD Android, with all Android releases from CAF using the Linux kernel, in a qbt1000 ioctl handler, an incorrect buffer size check has an integer overflow vulnerability potentially leading to a buffer overflow. **CVE ID : CVE 2017-9690**	https://source.android.com/security/bulletin/2017-11-01	O-GOO-ANDRO-11217/73
NA	16-11-2017	7.5	An elevation of privilege vulnerability in the Android media framework (mediaanalytics). Product: Android. Versions: 8.0. Android ID: A-65540999. **CVE ID : CVE 2017-0847**	https://source.android.com/security/bulletin/pixel/2017-11-01	O-GOO-ANDRO-11217/74
NA	16-11-2017	9.3	In android for MSM, Firefox OS for MSM, QRD Android, with all Android releases from CAF using the Linux kernel, in the KGSL driver function kgsl_ioctl_gpu_command, a Use After Free condition can potentially occur. **CVE ID : CVE 2017-11092**	https://source.android.com/security/bulletin/2017-11-01	O-GOO-ANDRO-11217/75
Overflow	16-11-2017	9.3	In android for MSM, Firefox OS for	https://source.	O-GOO-

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	Patch	NCIIPC ID
			MSM, QRD Android, with all Android releases from CAF using the Linux kernel, currently, the value of SIR_MAC_AUTH_CHALLENGE_LENGTH is set to 128 which may result in buffer overflow since the frame parser allows challenge text of length up to 253 bytes, but the driver can not handle challenge text larger than 128 bytes. **CVE ID : CVE 2017-11015**	android.com/security/bulletin/2017-11-01	ANDRO-11217/76
Overflow	16-11-2017	9.3	In android for MSM, Firefox OS for MSM, QRD Android, with all Android releases from CAF using the Linux kernel, while parsing a Measurement Request IE in a Roam Neighbor Action Report, a buffer overflow can occur. **CVE ID : CVE 2017-11014**	https://source.android.com/security/bulletin/2017-11-01	O-GOO-ANDRO-11217/77
NA	16-11-2017	9.3	In android for MSM, Firefox OS for MSM, QRD Android, with all Android releases from CAF using the Linux kernel, countOffset (in function UnpackCore) is increased for each loop, while there is no boundary check against "pIe->arraybound". **CVE ID : CVE 2017-11013**	https://source.android.com/security/bulletin/2017-11-01	O-GOO-ANDRO-11217/78
Execute Code	16-11-2017	9.3	A remote code execution vulnerability in the Android media framework (libmpeg2). Product: Android. Versions: 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2, 8.0. Android ID: A-63316832. **CVE ID : CVE 2017-0835**	https://source.android.com/security/bulletin/2017-11-01	O-GOO-ANDRO-11217/79
Execute Code	16-11-2017	9.3	A remote code execution vulnerability in the Android media framework (libmpeg2). Product: Android. Versions: 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2, 8.0. Android ID: A-63125953. **CVE ID : CVE 2017-0834**	https://source.android.com/security/bulletin/2017-11-01	O-GOO-ANDRO-11217/80
Execute Code	16-11-2017	9.3	A remote code execution vulnerability in the Android media	https://source.android.com/se	O-GOO-ANDRO-

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	Patch	NCIIPC ID
			framework (libavc). Product: Android. Versions: 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2, 8.0. Android ID: A-62896384. **CVE ID : CVE 2017-0833**	curity/bulletin/ 2017-11-01	11217/81
Execute Code	16-11-2017	9.3	A remote code execution vulnerability in the Android media framework (libmpeg2). Product: Android. Versions: 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2, 8.0. Android ID: A-62887820. **CVE ID : CVE 2017-0832**	https://source.android.com/security/bulletin/ 2017-11-01	O-GOO-ANDRO-11217/82
NA	16-11-2017	9.3	An elevation of privilege vulnerability in the Android framework (window manager). Product: Android. Versions: 8.0. Android ID: A-37442941. **CVE ID : CVE 2017-0831**	https://source.android.com/security/bulletin/ 2017-11-01	O-GOO-ANDRO-11217/83
NA	16-11-2017	9.3	An elevation of privilege vulnerability in the Android framework (device policy client). Product: Android. Versions: 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2, 8.0. Android ID: A-62623498. **CVE ID : CVE 2017-0830**	https://source.android.com/security/bulletin/ 2017-11-01	O-GOO-ANDRO-11217/84
Moxa					
Eds-g512e Firmware					
XSS	17-11-2017	3.5	An issue was discovered on MOXA EDS-G512E 5.1 build 16072215 devices. There is XSS in the administration interface. **CVE ID : CVE 2017-13700**	https://www.sentryo.net/fr/sentryo-analyse-switch-industriel/	O-MOX-EDS-G-11217/85
Gain Information	17-11-2017	5	An issue was discovered on MOXA EDS-G512E 5.1 build 16072215 devices. Cookies can be stolen, manipulated, and reused. **CVE ID : CVE 2017-13702**	https://www.sentryo.net/fr/sentryo-analyse-switch-industriel/	O-MOX-EDS-G-11217/86
DoS	17-11-2017	7.8	An issue was discovered on MOXA EDS-G512E 5.1 build 16072215 devices. A denial of service may occur. **CVE ID : CVE 2017-13703**	https://www.sentryo.net/fr/sentryo-analyse-switch-industriel/	O-MOX-EDS-G-11217/87

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;

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;							