Security Advisory | Volume 2018-07-01

CautelaLabs

PRODUCT	DESCRIPTION	AFFECTED VERSIONS	OTHER INFORMATION
[cisco-sa-20180620-nx-os-fabric-dos] Cisco NX-OS and FX-OS Remote Information Disclosure or DoS Vulnerability - CVE-2018-0310	A vulnerability in the Cisco Fabric Services component of Cisco FXOS Software and Cisco NX-OS Software could allow an unauthenticated, remote attacker to obtain sensitive information from memory or cause a denial of service (DoS) condition on the affected product. The vulnerability exists because the affected software insufficiently validates header values in Cisco Fabric Services packets. An attacker could exploit this vulnerability by sending a crafted Cisco Fabric Services packet to an affected device. A successful exploit could allow the attacker to cause a buffer overread condition, which could allow the attacker to obtain sensitive information from memory or cause a DoS condition on the affected product. This vulnerability affects Firepower 4100 Series Next-Generation Firewalls, Firepower 9300 Security Appliance, MDS 9000 Series Multilayer Switches, Nexus 2000 Series Fabric Extenders, Nexus 3000 Series Switches, Nexus 3500 Platform Switches, Nexus 5500 Platform Switches, Nexus 5600 Platform Switches, Nexus 6000 Series Switches, Nexus 7000 Series Switches, Nexus 7700 Series Switches, Nexus 9000 Series Switches in standalone NX-OS mode, Nexus 9500 R-Series Line Cards and Fabric Modules, UCS 6100 Series Fabric Interconnects, UCS 6200 Series Fabric Interconnects, UCS 6300 Series Fabric Interconnects. Cisco Bug IDs: CSCvd69957, CSCve02435, CSCve04859, CSCve41536, CSCve41538, CSCve41559	Version(s): <= FX-OS, NX-OS	Published - June 20, 2018 CVE-2018-0310 CVSS - 9.1 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0310 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0310 http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180620-nx-os-fabric-dos
Apple MacOS X <10.13.3 Authentication Bypass Vulnerability in Security - CVE-2017-13889	Apple MacOS X before 10.13.3 is prone to an authentication bypass vulnerability that could allow a non administrator attacker to bypass the administrator authentication.	Version(s): <= 10.13.3	Published - June 21, 2018 CVE-2017-13889 CVSS - 9.8 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-13889 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-13889 https://support.apple.com/en-us/HT208465
Jetty Remote Privilege Escalation Vulnerability - CVE-2018-12538	In Eclipse Jetty versions 9.4.0 through 9.4.8, when using the optional Jetty provided FileSessionDataStore for persistent storage of HttpSession details, it is possible for a malicious user to access/hijack other HttpSessions and even delete unmatched HttpSessions present in the FileSystem's storage for the FileSessionDataStore	Version(s): <= 9.4.0-9.4.8	Published - June 22, 2018 CVE-2018-12538 CVSS - 9.8 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-12538 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-12538
Linux Kernel 4.17.2 and Earlier Remote DoS or Other Impact Vulnerability - CVE-2018-12714	An issue was discovered in the Linux kernel through 4.17.2. The filter parsing in kernel/trace/trace_events_filter.c could be called with no filter, which is an N=0 case when it expected at least one line to have been read, thus making the N-1 index invalid. This allows attackers to cause a denial of service (slab out-of-bounds write) or possibly have unspecified other impact via crafted perf_event_open and mmap system calls.	Version(s): <= 4.17.2	Published - June 24, 2018 CVE-2018-12714 CVSS - 9.8 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-12714 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-12714 http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=81f9c4e4177d31ced6f52a89bb70e93bfb77ca03
DIGISOL DG-BR4000NG Remote Buffer Overflow Vulnerability - CVE-2018-12706	DIGISOL DG-BR4000NG devices have a Buffer Overflow via a long Authorization HTTP header	Version(s): <= *	Published - June 24, 2018 CVE-2018-12706 CVSS - 9.8 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-12706 https://hackings8n.blogspot.com/2018/06/cve-2018-12706-digisol-dg-br4000ng.html
Jenkins CollabNet Plugin Man-in-the-Middle Vulnerability - CVE-2018-1000605	A man in the middle vulnerability exists in Jenkins CollabNet Plugin 2.0.4 and earlier in CollabNetApp.java, CollabNetPlugin.java, CNFormFieldValidator.java that allows attackers to impersonate any service that Jenkins connects to.	Version(s): <= 2.0.4	Published - June 26, 2018 CVE-2018-1000605 CVSS - 9.8 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1000605 https://jenkins.io/security/advisory/2018-06-25/SECURITY-941
H2O Remote Code Execution or DoS Vulnerability - CVE-2018-0608	Buffer overflow in H2O version 2.2.4 and earlier allows remote attackers to execute arbitrary code or cause a denial of service (DoS) via unspecified vectors.	Version(s): <= 2.2.4	Published - June 26, 2018 CVE-2018-0608 CVSS - 9.8 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0608 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0608
Mozilla Firefox <61, ESR <52.9, ESR 60.0 and Thunderbird <52.9 Remote CSRF via 307 Redirects and NPAPI Plugins - CVE-2018-12364	Mozilla Firefox before 61, Firefox ESR before 52.9 and 60 before 60.1 and Thunderbird <52.9 could allow a malicious site to conduct a cross-site request forgery attack, via NPAPI plugins that can bypass CORS by making a certain same-origin POST request.	Version(s): <= 60.0 ESR-60.0.99 ESR, <61 relese, <52.9ESR	Published - June 26, 2018 CVE-2018-12364 CVSS - 9.6 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-12364 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-12364 https://www.mozilla.org/en-US/security/advisories/mfsa2018-15/
Linux Kernel 4.15.0 Remote DoS or Other Impact Vulnerability - CVE-2018-12931	ntfs_attr_find in the ntfs.ko filesystem driver in the Linux kernel 4.15.0 allows attackers to trigger a stack-based out-of-bounds write and cause a denial of service (kernel oops or panic) or possibly have unspecified other impact via a crafted ntfs filesystem.	Version(s): <= 4.15.0	Published - June 28, 2018 CVE-2018-12931 CVSS - 9.8 Vendor's Advisory - http://www.securityfocus.com/bid/104588 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-12931 https://bugs.launchpad.net/ubuntu/+source/linux/+bug/1763403
Apache Cassandra Remote Code Execution Vulnerability via RMI Request - CVE-2018-8016	The default configuration in Apache Cassandra 3.8 through 3.11.1 binds an unauthenticated JMX/RMI interface to all network interfaces, which allows remote attackers to execute arbitrary Java code via an RMI request. This issue is a regression of CVE-2015-0225. The regression was introduced in https://issues.apache.org/jira/browse/CASSANDRA-12109. The fix for the regression is implemented in https://issues.apache.org/jira/browse/CASSANDRA-14173. This fix is contained in the 3.11.2 release of Apache Cassandra.	Version(s): <= 3.8-3.11.1	Published - June 28, 2018 CVE-2018-8016 CVSS - 9.8 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-8016 https://lists.apache.org/thread.html/bafb9060bbdf958a1c15ba66c68531116fba4a83858a2796254da066@%3Cuser.cassandra.apache.org%3E