PRODUCT	DESCRIPTION	AFFECTED VERSIONS	OTHER INFORMATION
Adobe ColdFusion 11 and 2016 Remote Code Execution Vulnerability	Adobe ColdFusion 11 before update 14, and 2016 before update 6 is prone to a remote code execution vulnerability due to deserialization of untrusted data.	Version(s): <= 11- 11 update 14, 2016-2016 update 5	Published - April 10, 2018 CVE-2018-4939 CVSS - 9.8 Vendor's Advisory - https://helpx.adobe.com/security/products/coldfusion/apsb18-14.html http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-4939
Cisco IOS XE Remote Restrictions Bypass Vulnerability	A vulnerability in Cisco IOS XE Software could allow an unauthenticated, remote attacker to log in to a device running an affected release of Cisco IOS XE Software with the default username and password that are used at initial boot, aka a Static Credential Vulnerability. The vulnerability is due to an undocumented user account with privilege level 15 that has a default username and password. An attacker could exploit this vulnerability by using this account to remotely connect to an affected device. A successful exploit could allow the attacker to log in to the device with privilege level 15 access. This vulnerability affects Cisco devices that are running a vulnerable release of Cisco IOS XE Software Release 16.x. This vulnerability does not affect Cisco IOS XE Software releases prior to Release 16.x. Cisco Bug IDs: CSCve89880.	Version(s): <= 16.5.1, 16.5.1a, Everest-16.5.1, 16.5.1b	Published - March 25, 2018 CVE-2018-0150 CVSS - 9.8 Vendor's Advisory - https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180328-xesc http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0150
Apple MacOS X <10.13.4 Remote Command Injection Vulnerability in Terminal	Apple MacOS X before 10.13.4 is prone to an arbitrary command execution spoofing vulnerability in Terminal. A remote attacker could exploit this issue by pasting malicious content.	Version(s): <= 10.13.4	Published - March 29, 2018 CVE-2018-4106 CVSS - 9.8 Vendor's Advisory - https://support.apple.com/en-il/HT208692 https://nvd.nist.gov/vuln/detail/CVE-2018-4106
Apple Xcode <9.3 Remote Unspecified Vulnerability in LLVM	Apple Xcode before 9.3 is prone to multiple unspecified issues in LLVM.	Version(s): <9.3	Published - March 29, 2018 CVE-2018-4164 CVSS - 9.8 Vendor's Advisory - https://support.apple.com/en-us/HT208699 https://nvd.nist.gov/vuln/detail/CVE-2018-4164
Apple iOS <11.3 Remote Code Execution Vulnerability in Telephony	Apple iOS before 11.3 is prone to a remote code execution vulnerability in Telephony due to a buffer overflow issue. A remote attacker could exploit this issue to execute arbitrary code on the affected system.	Version(s): <11.3	Published - March 30, 2018 CVE-2018-4148 CVSS - 9.8 Vendor's Advisory - https://support.apple.com/en-il/HT208693 https://nvd.nist.gov/vuln/detail/CVE-2018-4148
Cisco IOS, IOS XE Remote Code Execution or DoS via Crafted Smart Install Message	A vulnerability in the Smart Install feature of Cisco IOS Software and Cisco IOS XE Software could allow an unauthenticated, remote attacker to trigger a reload of an affected device, resulting in a denial of service (DoS) condition, or to execute arbitrary code on an affected device. The vulnerability is due to improper validation of packet data. An attacker could exploit this vulnerability by sending a crafted Smart Install message to an affected device on TCP port 4786. A successful exploit could allow the attacker to cause a buffer overflow on the affected device. Cisco Bug ID: CSCvg76186.	Version(s): Cisco IOS version 15.2(2)E8, 15.2(4)E6, 15.2(6)E1 and IOS XE Software version 3.6.8E, 3.8.6E, 3.10.1E,16.3.6, 16.4.2, 16.5.1b	Published - March 28, 2018 CVE-2018-0171 CVSS - 9.8 Vendor's Advisory - https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170214-smi https://nvd.nist.gov/vuln/detail/CVE-2018-0171 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0171
Cisco IOS and IOS XE Quality of Service Remote Code Execution Vulnerability	A vulnerability in the quality of service (QoS) subsystem of Cisco IOS Software and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with elevated privileges. The vulnerability is due to incorrect bounds checking of certain values in packets that are destined for UDP port 18999 of an affected device. An attacker could exploit this vulnerability by sending malicious packets to an affected device. When the packets are processed, an exploitable buffer overflow condition may occur. A successful exploit could allow the attacker to execute arbitrary code on the affected device with elevated privileges. The attacker could also leverage this vulnerability to cause the device to reload, causing a temporary DoS condition while the device is reloading. The malicious packets must be destined to and processed by an affected device. Traffic transiting a device will not trigger the vulnerability. Cisco Bug IDs: CSCvf73881.	Version(s):Cisco IOS 15.7(3)M1, 15.6(3)M4, 15.6(2)SP3b, 15.6(2)SP4 and IOS-XE version 3.16.7S, 3.6.6E, 16.6.2, 3.18.3bSP, 16.5.3, 16.4.3, 16.3.6	Published - March 28, 2018 CVE-2018-0151 CVSS - 9.8 Vendor's Advisory - https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180328-qos http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0151 https://nvd.nist.gov/vuln/detail/CVE-2018-0151
Drupal Remote Code Execution Vulnerability	Drupal before 7.58, 8.x before 8.3.9, 8.4.x before 8.4.6, and 8.5.x before 8.5.1 allows remote attackers to execute arbitrary code because of an issue affecting multiple subsystems with default or common module configurations.	Version(s): before 7.58, 8.x before 8.3.9, 8.4.x before 8.4.6, and 8.5.x before 8.5.1	Published - March 28, 2018 CVE-2018-7600 CVSS - 9.8 Vendor's Advisory - https://www.drupal.org/sa-core-2018-002 https://nvd.nist.gov/vuln/detail/CVE-2018-7600
Wireshark Unspecified Vulnerability in Ui/failure_message.c	In Wireshark 2.4.0 to 2.4.5 and 2.2.0 to 2.2.13, ui/failure_message.c has a memory leak.	Version(s):2.4.0 - 2.4.5, 2.2.0 - 2.2.13	Published - April 03, 2018 CVE-2018-9274 CVSS - 9.8 Vendor's Advisory - https://www.wireshark.org/security/wnpa-sec-2018-24.html https://nvd.nist.gov/vuln/detail/CVE-2018-9274
SAP Business Client 6.5 Code Execution, DoS, or Other Vulnerability due to Memory Corruption	SAP Business Client 6.5 is vulnerable to attackers executing commands, performing a denial of service, or other unspecified effects.	Version(s): 6.5	Published - April 10, 2018 SBV-84172 CVSS - 9.8 Vendor's Advisory - https://blogs.sap.com/2018/04/10/sap-security-patch-day-april-2018/ https://erpscan.com/press-center/blog/sap-cyber-threat-intelligence-report-april-2018/

PRODUCT	DESCRIPTION	AFFECTED VERSIONS	OTHER INFORMATION
		Version(s): <= 7.20.0-7.58.0	Published - March 14, 2018 CVE-2018-1000122 CVSS - 8.2 Vendor's Advisory - http://www.securityfocus.com/bid/103436 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1000122 https://curl.haxx.se/docs/adv_2018-b047.html