PRODUCT	DESCRIPTION	AFFECTED VERSIONS	OTHER INFORMATION
Red Hat JBoss Enterprise Application Platform 7 Remote Password Hash Disclosure via a Timing Attack - CVE-2014-9970	Red Hat JBoss Enterprise Application Platform 7 Remote Password Hash Disclosure via a Timing Attack - CVE-2014-9970 jasypt, as used in Red Hat JBoss Enterprise Application Platform 7, allows a timing attack against the password hash comparison.	Version(s): <= 7.0 EL7, 7.0 EL6, 7.0	Published - September 29, 2017 CVE-2017-2808, 2809, 2811 CVSS - 7.5 Vendor's Advisory - https://access.redhat.com/errata/RHSA-2017:2808 https://access.redhat.com/errata/RHSA-2017:2809 https://access.redhat.com/errata/RHSA-2017:28011
Citrix NetScaler ADC Remote Privilege Elevation Vulnerability - CVE-2017-14602	Citrix NetScaler ADC Remote Privilege Elevation Vulnerability - CVE-2017-14602 Citrix NetScaler Application Delivery Controller (ADC) 10.1 before build 135.18, 10.5 before build 66.9, 10.5e before build 60.7010.e, 11.0 before build 70.16, 11.1 before build 55.13, and 12.0 before build 53.13 (except for build 41.24) are vulnerable to remote privilege elevation from their management interfaces. If exploited, this could allow an attacker with access to the NetScaler management interface to gain administrative access to the appliance.	Version(s): < = 10.1 - 10.1 Build 135.17, 11.0 - 11.0 Build 70.15, 12.0 -12.0 Build 53.12, 11.1 - 11.1 Build 55.12, 10.5e - 10.5eBuild 60.7009.e, 10.5 -10.5 Build 66.8	Published - October 3, 2017 CVE-2017-14602 CVSS - 9.8 Vendor's Advisory - https://www.citrix.com/downloads/netscaler-adc/
Apple tvOS <11 Remote Unspecified Vulnerability in zlib - CVE-2016-9843	Apple tvOS <11 Remote Unspecified Vulnerability in zlib - CVE-2016-9843 zlib, as used in Apple tvOS before 11, is prone to a remote unspecified vulnerability via vectors involving big-endian CRC calculation. A remote attacker could exploit this issue to cause an unspecified impact on the affected system.	Version(s): < 11	Published - September 25, 2017 CVE-2016-9843 CVSS - 9.8 Vendor's Advisory - http://www.securityfocus.com/bid/95131 https://support.apple.com/en-il/HT208113 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-9843 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-9843
Citrix NetScaler Gateway Remote Privilege Elevation Vulnerability - CVE-2017-14602	Citrix NetScaler Gateway Remote Privilege Elevation Vulnerability - CVE-2017-14602 Citrix NetScaler Application Delivery Controller (ADC) 10.1 before build 135.18, 10.5 before build 66.9, 10.5e before build 60.7010.e, 11.0 before build 70.16, 11.1 before build 55.13, and 12.0 before build 53.13 (except for build 41.24) are vulnerable to remote privilege elevation from their management interfaces. If exploited, this could allow an attacker with access to the NetScaler management interface to gain administrative access to the appliance.	Version(s): < = 10.1 - 10.1 Build 135.17, 11.0 - 11.0 Build 70.15, 12.0 -12.0 Build 53.12, 11.1 - 11.1 Build 55.12, 10.5e - 10.5eBuild 60.7009.e, 10.5 -10.5 Build 66.8.	Published - October 3, 2017 CVE-2017-14602 CVSS - 9.8 Vendor's Advisory - https://www.citrix.com/downloads/netscaler-gateway/ http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-14602
[cisco-sa-20170927-dhcp] Cisco IOS and IOS-XE Remote Code Execution or DoS Vulnerability - CVE-2017-12240	[cisco-sa-20170927-dhcp] Cisco IOS and IOS-XE Remote Code Execution or DoS Vulnerability - CVE-2017-12240 The DHCP relay subsystem of Cisco IOS 12.2 through 15.6 and Cisco IOS XE Software contains a vulnerability that could allow an unauthenticated, remote attacker to execute arbitrary code and gain full control of an affected system. The attacker could also cause an affected system to reload, resulting in a denial of service (DoS) condition. The vulnerability is due to a buffer overflow condition in the DHCP relay subsystem of the affected software. An attacker could exploit this vulnerability by sending a crafted DHCP Version 4 (DHCPv4) packet to an affected system. A successful exploit could allow the attacker to execute arbitrary code and gain full control of the affected system or cause the affected system to reload, resulting in a DoS condition. Cisco Bug IDs: CSCsm45390, CSCuw77959.	Version(s): < = 02.01.00 - 02.06.02, 3.1.0S - 3.5.2S	"Published - October 2, 2017 CVE-2017-12240 CVSS - 9.8 Vendor's Advisory - http://www.securityfocus.com/bid/101034 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-12240 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170927-dhcp
[cisco-sa-20170927-privesc] Cisco IOS XE Privilege Escalation Vulnerability - CVE-2017-12230	[cisco-sa-20170927-privesc] Cisco IOS XE Privilege Escalation Vulnerability - CVE-2017-12230 A vulnerability in the web-based user interface (web UI) of Cisco IOS XE 16.2.1 and Denali-16.3.1 could allow an authenticated, remote attacker to elevate their privileges on an affected device. The vulnerability is due to incorrect default permission settings for new users who are created by using the web UI of the affected software. An attacker could exploit this vulnerability by using the web UI of the affected software to create a new user and then logging into the web UI as the newly created user. A successful exploit could allow the attacker to elevate their privileges on the affected device. This vulnerability affects Cisco devices that are running a vulnerable release Cisco IOS XE Software, if the HTTP Server feature is enabled for the device. The newly redesigned, web-based administration UI was introduced in the Denali 16.2 Release of Cisco IOS XE Software. This vulnerability does not affect the web-based administration UI in earlier releases of Cisco IOS XE Software. Cisco Bug IDs: CSCuy83062.	Version(s): < = 16.2.1, Denail-16.3.1	Published - October 1, 2017 CVE-2017-12230 CVSS - 9.9 Vendor's Advisory - https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170927-privesc http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-12230
Apple MacOS X <10.13 Remote Unspecified Vulnerability in zlib - CVE-2016-9843	Apple MacOS X <10.13 Remote Unspecified Vulnerability in zlib - CVE-2016-9843 Apple MacOS X before 10.13 is prone to a remote unspecified vulnerability in zlib. A remote attacker could exploit this issue to cause an unspecified impact on the affected system.	Version(s): <= 10.13	Published - October 2, 2017 CVE-2016-9843 CVSS - 9.8 Vendor's Advisory - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-9843 https://support.apple.com/en-il/HT208144
Apple MacOS X <10.13 Remote Unspecified Vulnerability in zlib - CVE-2016-9841	Apple MacOS X <10.13 Remote Unspecified Vulnerability in zlib - CVE-2016-9841 Apple MacOS X before 10.13 is prone to a remote unspecified vulnerability in zlib. A remote attacker could exploit this issue to cause an unspecified impact on the affected system.	Version(s) :<= 10.13	Published - October 02, 2017 CVE-2016-9841. CVSS - 9.8 Vendor's Advisory - https://support.apple.com/en-il/HT208144 http://www.securityfocus.com/bid/95131