PRODUCT	DESCRIPTION	AFFECTED VERSIONS	OTHER INFORMATION
IBM Platform Symphony and Spectrum Symphony Remote Information Disclosure or DoS Vulnerability - CVE-2018-1702	IBM Platform Symphony 7.1 Fix Pack 1 and 7.1.1 and IBM Spectrum Symphony 7.1.2 and 7.2.0.2 are vulnerable to a XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 146189.	Spectrum Symphony Version(s): <= 7.1.2, 7.2.02. Platform Symphony Version(s): <=7.1.1, 7.1 Fix Pack1	Published - Sep 30, 2018 CVE- 2018-1702 CVSS - 7.1 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1702 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-1702
[APSB18-30] Adobe Acrobat and Reader Remote Code Execution Vulnerability - CVE-2018-15940	Adobe Acrobat and Reader DC Continuous through 2018.011.20063, Acrobat and Reader Classic 2017 through 2017.011.30102, and Adobe Acrobat and Reader DC Classic 2015 through 2015.006.30452 are prone to remote code execution due to an out-of-bounds write vulnerability.	Reader 2017 Version(s): =< 2017.011.30102 Acrobat 2017 Version(s): =< 2017.011.30102	Published - Oct 08, 2018 CVE- 2018-15940 CVSS - 8.8 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-15940 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-15940
Apple MacOS X <10.13.4 Remote Privilege Elevation Vulnerability in CoreFoundation - CVE-2017-7151	Apple MacOS X before 10.13.4 is prone to a remote privilege elevation vulnerability in CoreFoundation. A remote attacker could exploit this issue to gain privileges on the affected system via a crafted application.	Version(s): <10.13.4	Published - Oct 02, 2018 CVE- 2018-7151 CVSS - 7.8 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7151 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-7151
Mozilla Firefox <62.0.3, Firefox ESR <60.2.2 Local Code Execution Vulnerability - CVE-2018-12386	Mozilla Firefox before 62.0.3, and Firefox ESR before 60.2.2 are prone to remote code execution vulnerability due to weakness in JavaScript register allocation which could lead to type confusion and, consecutively to arbitrary read and write.	Firefox Internet & Mobile Version(s): < 62.03, 60.2.2 ESR Enterprise Linux Server Redhat Version = 6, 7, EUS 7.5 Enterprise Linux Workstation Redhat Version = 6, 7	Published - Oct 09, 2018 CVE- 2018-12386 CVSS - 8.4 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-12386 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-12386
Apple MacOS X <10.13.2 Remote DoS Vulnerability in Perl - CVE-2017-12837	Perl 5, as used in Apple MacOS X before 10.13.2, is vulnerable to a heap-based buffer overflow in the S_regatom function in regcomp.c, which allows remote attackers to cause a denial of service (out-of-bounds write) via a regular expression with a '\N{}' escape and the case-insensitive modifier.	Version(s): < 10.13.2	Published - Oct 07, 2018 CVE- 2018-12837 CVSS - 7.5 Vendor's Advisory - http://www.securityfocus.com/bid/100860 https://support.apple.com/en-us/HT208331
RedHat JBoss Enterprise Web Server <5.0 SP1 Remote Information Disclosure Vulnerability in Tomcat - CVE-2018-8037	Apache Tomcat, as used in RedHat JBoss Enterprise Web Server before 5.0 Service Pack 1, is vulnerable to remote information disclosure. If an async request was completed by the application at the same time as the container triggered the async timeout, a race condition existed that could result in a user seeing a response intended for a different user. An additional issue was present in the NIO and NIO2 connectors that did not correctly track the closure of the connection when an async request was completed by the application and timed out by the container at the same time. This could also result in a user seeing a response intended for another user.	Version(s): < 5.0 SP1, 5 EL6, 5EL7	Published - Oct 04, 2018 CVE- 2018-8037 CVSS - 9.1 Vendor's Advisory - http://www.securityfocus.com/bid/104894 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-8037
[cisco-sa-20181003-webex-rce] Cisco WebEx Network Recording Player, WebEx Player Remote Code Execution Vulnerability - CVE-2018-15431	Cisco WebEx Network Recording Player for Microsoft Windows and Cisco Webex Player for Microsoft Windows included in Cisco Webex Meetings Suite WBS31, WBS32 before WBS32.15.30, WBS33, Cisco Webex Meetings Online before 1.3.38 and Cisco Webex Meetings Server before 3.0MR2 Patch 1 are prone to a remote code execution vulnerability due to a flaw in validation of Advanced Recording Format (ARF) and Webex Recording Format (WRF) files. A remote attacker could exploit these vulnerabilities by sending crafted ARF or WRF file via links or email attachments and convincing the user to open the file.	Version(s): = 33.*, 31.*, 32.0.0 - 32.15.29	Published - Oct 03, 2018 CVE- 2018 -15431 CVSS - 7.8 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-15431 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-15431
[cisco-sa-20181003-asa-dma-dos] Cisco ASA , FirePower Threat Defense Remote DoS Vulnerability - CVE-2018-15383	Cisco ASA versions 9.3.x and 9.4 before 9.4.4.22, 9.5.x and 9.6 before 9.6.4.14, 9.7.x and 9.8.x before 9.8.3.8, and 9.9.x before 9.9.2.18 are prone to a remote denial-of-service vulnerability due to inadequate handling of resources in low-memory conditions. An attacker could exploit the flaw by sending a high rate of traffic which would exhaust DMA memory and cause a reload and temporary denial-of-service.	ASA Version(s): = 9.4-9.4.4.21, 9.6-9.6.4.13, 9.3.*, 9.5.*, 9.9-9.9.2.17, 9.8-9.8.3.7 FTD Version = 6.2.2-6.2.2.5, 6.2.0 - 6.2.06, 6.2.3-6.2.3.3, 6.0-6.1.0.6	Published - Oct 09, 2018 CVE- 2018-15383 CVSS - 8.6 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-15383 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-15383
Apple MacOS X <10.13.4 Remote Privilege Elevation Vulnerability in CoreFoundation - CVE-2017-7151	Apple MacOS X before 10.13.4 is prone to a remote privilege elevation vulnerability in CoreFoundation. A remote attacker could exploit this issue to gain privileges on the affected system via a crafted application.	Version(s): < 10.13.4	Published - Oct 09, 2018 CVE- 2018-7151 CVSS - 7.8 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7151 https://support.apple.com/en-us/HT208331