PRODUCT	DESCRIPTION	AFFECTED VERSIONS	OTHER INFORMATION
Oracle Siebel Apps - Field Service Remote Code Execution Vulnerability in Smart Answer (Python) - CVE-2013-1903	PostgreSQL as used in Oracle Siebel Apps versions 16.0, 17.0 is prone to a remote code execution vulnerability. A remote unauthenticated attacker could exploit this issue to execute arbitrary code with kernel privileges on the affected system.	Version(s): <= 16.0, 17.0	Published - October 17, 2017 CVE-2013-1903 CVSS - 10.0 Vendor's Advisory - http://www.oracle.com/technetwork/topics/security/cpuoct2017-3236626.html http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-1903
Oracle Healthcare Master Person Index Remote Code Execution - CVE-2016-6814	Oracle Healthcare Master Person Index version 4.x is prone to a remote code execution vulnerability in Relationship Management (Apache Groovy). An unauthenticated remote attacker could exploit this issue to execute arbitrary code on the affected system.	Version(s): <= 4.*	Published - October 17, 2017 CVE-2016-6814 CVSS - 9.6 Vendor's Advisory - http://www.oracle.com/technetwork/topics/security/cpuoct2017-3236626.html http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-6814
Oracle BI Publisher Remote Code Execution Vulnerability in Apache ActiveMQ - CVE-2015-5254	Apache ActiveMQ, as used in Oracle BI Publisher 11.1.1.7.0, 12.2.1.1.0, and 12.2.1.2.0 does not restrict the classes that can be serialized in the broker, which allows remote attackers to execute arbitrary code via a crafted serialized Java Message Service (JMS) ObjectMessage object.	Version(s): <= 11.1.1.7.0, 12.2.1.1.0, 12.2.1.2.0	Published - October 17, 2017 CVE-2015-5254 CVSS - 9.8 Vendor's Advisory - http://www.oracle.com/technetwork/topics/security/cpuoct2017-3236626.html http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-5254
Juniper JunOS, ScreenOS, WLAN Remote Encryption Bypass Vulnerability in WPA/WPA2 Protocols (KRACK) - CVE-2017-13081	Juniper JunOS 12.1X46 on SRX 210, 240, 650 series firewalls which support AX411 access points, ScreenOS 6.3 on SSG-5 and SSG-20 firewalls with integrated Wi-Fi radios and the Wireless LAN controller 9.2 and 9.6 are prone to an encryption bypass vulnerability due to reinstallation of the group key (GTK) in the four-way handshake in the WPA and WPA2 protocols.	Version(s): <= 12.1X46 & 9.6, 9.2 (Wireless LAN controller)	Published - October 16, 2017 CVE-2017-13081 CVSS - 7.9 Vendor's Advisory - https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10827&actp=METADATA http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-13081
Adobe Flash Player 27.0.0.159/27.0.0.130 Remote Code Execution Vulnerability via Type Confusion - CVE-2017-11292	Adobe Flash Player Desktop Runtime for Windows, Macintosh, and Linux version 27.0.0.159, Adobe Flash Player for Microsoft Edge and Internet Explorer 11 version 27.0.0.159, and Adobe Flash Player for Google Chrome version 27.0.0.130 are vulnerable to remote code execution via type confusion. A remote attacker could exploit this by enticing a user to open a file with embedded malicious code.	Version(s): <= 27.0.0.159, 27.0.0.130	Published - October 16, 2017 CVE-2017-11292 CVSS - 8.8 Vendor's Advisory - https://www.adobe.com/software/flash/about/ http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11292
Cisco Remote Encryption Bypass Vulnerability in WPA/WPA2 Protocols (KRACK) - CVE-2017-13080	Multiple Cisco products are prone to an encryption bypass vulnerability due to improper session key negotiation in the four-way handshake in the WPA and WPA2 protocols. This weakness could lead to pairwise transient key, group key or integrity key reinstallation. Cisco Bug IDs: CSCvg35287, CSCvf71761, CSCvf71751, CSCvf71754, CSCvf71749, CSCvf47808, CSCvf96789, CSCvf96814, CSCvf96818.	Version(s): Wireless Access Point = 300, 500. AnyConnect Secure Mobility Client = 4.5(2033) IOS = 8.5(103.0) Wireless LAN Controller = 9.3(2), 9.4(2)TT1.2	Published - October 16, 2017 CVE-2017-13080 CVSS - 5.4 Vendor's Advisory - https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171016-wpa http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-13080
Apache Struts 2.0.0 - 2.3.28.1 Remote Code Execution Vulnerability - CVE-2016-4461	Apache Struts 2.0.0 - 2.3.28.1 is vulnerable to remote code execution via a "%{}" sequence in a tag attribute, aka forced double OGNL evaluation. This could allow a remote attacker to execute arbitrary code. NOTE: this vulnerability exists because of an incomplete fix for CVE-2016-0785.	Version(s): <= 2.0.0, 2.3.28.1	Published - October 16, 2017 CVE-2017-11292 CVSS - 7.3 Vendor's Advisory - https://www.adobe.com/software/flash/about/ http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-4461