Security Advisory | Volume 2018-12-01

PRODUCT	DESCRIPTION	AFFECTED VERSIONS	OTHER INFORMATION
Citrix XenServer Local Code Execution	Citrix XenServer versions 7.0, 7.1 LTSR CU1, 7.5 and 7.6 are prone to a code execution vulnerability. This vulnerability was published by Nessus	Version(s) Citrix Servers & Desktop OS 7.1 LTSR CU1, 7.0, 7.5, 7.6	Published - Nov 26, 2018 SBV-94489 CVSS - 9.3 Vendor's Advisory - https://support.citrix.com/article/CTX239432 https://www.tenable.com/plugins/nessus/119148
VMware Workstation, Fusion Remote Integer Overflow Vulnerability - CVE-2018-6983	IVMware Workstation 14.x before 14.1.5, and 15.x before 15.0.2, and VMware Fusion on Mac OS X 11.x before 11.0.2, and 10.x before 10.1.5 are prone to an integer overflow vulnerability in virtual network devices. The flaw could enable a guest to execute code on the host.	Version(s) VMWare Servers & Desktop OS 11.1.0, 11.1.1, 10.1.0, -10.1.4, 10.0*, 11.0*, 15..0.0, 15.0.1, 14.1.0-14.1.4, 14.0*	Published - Nov 23, 2018 CVE-2018-6983 CVSS - 9.8 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-6983 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-6983
cisco-sa-20181128-plm-sql-inject] Cisco Prime License Manager Remote SQL Injection Vulnerability - CVE-2018-15441	A vulnerability in the web framework code of Cisco Prime License Manager (PLM) could allow an unauthenticated, remote attacker to execute arbitrary SQL queries. The vulnerability is due to a lack of proper validation of user-supplied input in SQL queries. An attacker could exploit this vulnerability by sending crafted HTTP POST requests that contain malicious SQL statements to an affected application. A successful exploit could allow the attacker to modify and delete arbitrary data in the PLM database or gain shell access with the privileges of the postgres user.	Version(s) Cisco 11.0.1 - 11.5.1	Published - Nov28, 2018 CVE-2018-15441 CVSS - 9.8 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-15441 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-15441
Imperva SecureSphere Remote Code Execution Vulnerability - CVE-2018-19646	The Python CGI scripts in PWS in Imperva SecureSphere 13.0.10, 13.1.10, and 13.2.10 allow remote attackers to execute arbitrary OS commands because command-line arguments are mishandled.	Version(s): Imperva 13.0.10, 13.1.10, 13.2.10	Published - Nov 28, 2018 CVE-2018- 19646 CVSS - 9.8 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-19646 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-19646
F5 Multiple BigIP Products Remote Unspecified Vulnerability due to Node.js - CVE-2018-7159	Node.js component, as used in F5 BigIP products (LTM, AAM, AFM, Analytics, APM, ASM, DNS, Edge Gateway, FPS, GTM, Link Controller, PEM, WebAccelerator), ignores spaces in the `Content-Length` header, allowing input such as `Content-Length: 1 2` to be interpreted as having a value of `12`. When the flaw is exploited, it may cause the affected Node.js component to behave unexpectedly, and therefore has an impact on BigIP products.	Version(s): F5 Networking & Security 12.1.0 - 12.1.3, 13.0.0 - 13.1.1, 14.0.0, 11.5.1 - 11.6.3, 11.2.1 - 11.6.3	Published - Nov 29, 2018 CVE-2018-7159 CVSS - 9.8 Vendor's Advisory -http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-7159 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-7159
Google Kubernetes Remote Elevation of Privilege and Information Disclosure Vulnerability - CVE-2018-1002105	Google Kubernetes is prone to remote privilege escalation and information disclosure vulnerabilities. A connection to backend servers (such as aggregated API servers and kubelets) can be established through Kubernetes API server using specially crafted requests. This connection can be then used to send request to backed servers directly, authenticated with the Kubernetes API server's TLS credentials	Version(s): Google Business Apps 1.11 - 1.11.4, 1.12 - 1.12.2, 1.0 - 1.9.99, 1.10 - 1.10.10	Published - Dec 03, 2018 CVE-2018-1002105 CVSS - 9.8 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1002105 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-1002105
Apple Watch OS <5.1.2 Privilege Elevation Vulnerability in Kernel - CVE-2018-4435	Apple Watch OS before 5.1.2 is prone to a privilege elevation vulnerability in Kernel. An attacker could exploit this issue to gain privileges on the affected system via a crafted application.	Version(s): Apple IOT < 5.1.2	Published - Dec 06, 2018 CVE-2018-3180 CVSS - 8.8 Vendor's Advisory - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-4435 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-4435
PHP Remote Code Execution Vulnerability - CVE-2018-19518	University of Washington IMAP Toolkit 2007f on UNIX, as used in imap_open() in PHP and other products, launches an rsh command (by means of the imap_rimap function in c-client/imap4r1.c and the tcp_aopen function in osdep/unix/tcp_unix.c) without preventing argument injection, which might allow remote attackers to execute arbitrary OS commands if the IMAP server name is untrusted input (e.g., entered by a user of a web application) and if rsh has been replaced by a program with different argument semantics. For example, if rsh is a link to ssh (as seen on Debian and Ubuntu systems), then the attack can use an IMAP server name containing a "-oProxyCommand" argument.	Version(s): PHP Dev Tools <= 5.6.38, 7.0, 7.2, 7.3	Published - Nov 25, 2018 CVE-2018-19518 CVSS - 9.8 Vendor's Advisory - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-19518 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-19518 http://nvd.nist.gov/vuln/detail/CVE-2018-19518
IBM WebSphere Application Server Local Information Disclosure Vulnerability - CVE-2018-1957	IBM WebSphere Application Server versions 9.0.0.0 through 9.0.0.9 are prone to a vulnerability which enables sensitive information to be available due to mishandling of data by the application based on an incorrect return by the httpServletRequest#authenticate() API when an unprotected URI is accessed.	Version(s): IBM Business Apps 9.0.0.0 - 9.0.0.9	Published - Dec 06, 2018 CVE-2018-1957 CVSS - 4.0 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1957 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-1957