

PRODUCT	DESCRIPTION	AFFECTED VERSIONS	OTHER INFORMATION
IBM WebSphere Application Server Remote Information Disclosure and DoS Vulnerability - CVE-2018-1905	IBM WebSphere Application Server version 9.0 before 9.0.0.10 is vulnerable to a XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this issue to obtain sensitive information or cause a denial of service condition by consuming memory resources.	Version(s) IBM Business Apps 9.0.0.0-9.0.0.9	Published - Nov 20, 2018 CVE- 2018-1905 CVSS - 7.1 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1905 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-1905
Linux Kernel local Elevation of Privilege Vulnerability - CVE-2018-18955	In the Linux kernel 4.15.x through 4.19.x before 4.19.2, map_write() in kernel/user_namespace.c allows privilege escalation because it mishandles nested user namespaces with more than 5 UID or GID ranges. A user who has CAP_SYS_ADMIN in an affected user namespace can bypass access controls on resources outside the namespace, as demonstrated by reading /etc/shadow. This occurs because an ID transformation takes place properly for the namespaced-to-kernel direction but not for the kernel-to-namespaced direction.	Version(s) Linux Servers & Desktop OS 4.15-4.19.1	Published - Nov 16, 2018 CVE-2018-18955 CVSS - 8.4 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-18955 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-18955
Google Chrome <70.0.3538.110 Unspecified Vulnerability in GPU - CVE-2018-17479	Google Chrome before 70.0.3538.110 is vulnerable to an unspecified vulnerability in the GPU component due to a use-after-free issue.	Version(s) Google Internet & Mobile <70.0.3538.110	Published - Nov 19, 2018 CVE-2018-17479 CVSS - 8.8 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-17479 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-17479
Dell EMC Avamar and Integrated Data Protection Appliance Remote Code Execution Vulnerability - CVE-2018-11066	The Dell EMC Avamar Client Manager in Dell EMC Avamar Server versions 7.2.0, 7.2.1, 7.3.0, 7.3.1, 7.4.0, 7.4.1, 7.5.0, 7.5.1, 18.1 and Dell EMC Integrated Data Protection Appliance (IDPA) versions 2.0, 2.1 and 2.2 is prone to a Remote Code Execution vulnerability.	Version(s): EMC Servers & Desktops 2.0, 2.1, 2.2 Version(s): EMC Business Apps 7.2.0, 7.2.1, 7.3.0, 7.3.1, 7.4.0, 7.4.1, 7.5.0, 7.5.1, 18.1	Published - Nov 20, 2018 CVE-2018-11066 CVSS - 9.8 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-11066 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-11066
VMWare vSphere Data Protection 6.0 - 6.0.8, 6.1 - 6.1.9 Remote Code Execution Vulnerability - CVE-2018-11066	VMWare vSphere Data Protection 6.0 before 6.0.9, and 6.1 before 6.1.10 is prone to a remote code execution vulnerability. A remote unauthenticated attacker could exploit this issue to execute arbitrary commands on the server.	Version(s): VMWare Networking & Security 6.0.0-6.0.8, 6.1.0-6.1.9	Published - Nov 20, 2018 CVE-2018-11066 CVSS - 9.8 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-11066 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-11066
Apple iOS 12.1 Just-In-Time Vulnerability in Safari Web Browser	Apple iOS 12.1 is prone to a just-in-time vulnerability in the Safari web browser. The vulnerability was found at the Pwn2Own 2018 mobile hacking competition.	Version(s): Apple Internet & Mobile 12.1	Published - Nov 14, 2018 SBV-93889 CVSS - 8.4 Vendor's Advisory - https://thehackernews.com/2018/11/mobile-hacking-exploits.html
IBM WebSphere Application Server Remote Unspecified Vulnerability in Java - CVE-2018-3180	An unspecified vulnerability related to the Java SE JSSE component, as used in IBM WebSphere Application Server Liberty through 18.0.0.3, IBM WebSphere Application Server Traditional Version 9.0.0.0 through 9.0.0.9, 8.5.0.0 through 8.5.5.14, 8.0.0.0 through 8.0.0.15, and 7.0.0.0 through 7.0.0.45, could allow an unauthenticated attacker to cause low confidentiality impact, low integrity impact, and low availability impact.	Version(s): IBM Business Apps <= 18.0.0.3, 8.0.0.0-8.0.0.15, 8.5.0.0-8.5.5.14, 9.0.0.0-9.0.0.9, 7.0.0.0-.7.0.0.45	Published - Nov 19, 2018 CVE-2018-3180 CVSS - 5.6 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-3180
Linux Kernel 4.19.2 and Earlier Local DoS Vulnerability - CVE-2018-19407	The vcpu_scan_ioapic function in arch/x86/kvm/x86.c in the Linux kernel through 4.19.2 allows local users to cause a denial of service (NULL pointer dereference and BUG) via crafted system calls that reach a situation where ioapic is uninitialized.	Version(s): Linux Server & Desktop OS <= 4.19.2	Published - Nov 21, 2018 CVE- 2018-19407 CVSS - 5.5 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-19407 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-19407
[APSB18-44] Adobe Flash Player <31.0.0.153 Remote Code Execution Vulnerability - CVE-2018-15981	A type confusion issue was discovered in Adobe Flash Player before 31.0.0.153. A remote attacker could exploit this issue to execute arbitrary code on the system.	Version(s): RedHat Servers & Desktop 6 Adobe Internet & mobile <=31.0.0.148	Published - Nov 20, 2018 CVE- 2018-15981 CVSS - 8.8 Vendor's Advisory - https://qualysguard.qualys.com/fo/common/vuln_info.php?allow_modify=1&id=371330 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-15981