Security Advisory | Volume 2018-009

PRODUCT	DESCRIPTION	AFFECTED VERSIONS	OTHER INFORMATION
Linux Kernel 4.14.10 and Earlier Remote Use-After-Free Vulnerability - CVE-2017-17975	Use-after-free in the usbtv_probe function in drivers/media/usb/usbtv/usbtv-core.c in the Linux kernel through 4.14.10 allows attackers to cause a denial of service (system crash) or possibly have unspecified other impact by triggering failure of audio registration, because a kfree of the usbtv data structure occurs during a usbtv_video_free call, but the usbtv_video_fail label's code attempts to both access and free this data structure.	Version(s): <= 4.14.10	Published - December 30, 2017 CVE-2017-17975 CVSS - 9.8 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-17975 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-17975
IBM Tivoli Monitoring DoS and Information Disclosure Vulnerability - CVE-2017-1289	IBM Tivoli Monitoring is prone to a denial-of-service and information disclosure vulnerability due to an XML external entity injection (XXE) error in IBM Java.	Version(s): <= 6.2.3 Fix Pack 01 - 6.3.0 Fix Pack 07	Published - December 28, 2017 CVE-2017-1289 CVSS - 8.2 Vendor's Advisory - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-1289 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-1289
Apple MacOS X <=10.13.1 Local Root Privilege Elevation Vulnerability in IOHIDSystem	Apple MacOS X 10.13.1 and earlier is vulnerable to local privilege elevation in IOHIDSystem. A local authenticated attacker could gain root privilege on the affected system. This vulnerability was published by Qualys.	Version(s): <= 10.13.1	Published - December 31, 2017 SBV-79905 CVSS - 7.8 Vendor's Advisory - https://siguza.github.io/IOHIDeous/ https://github.com/Siguza/IOHIDeous/
VMware vSphere Data Protection Remote Escalation of Privileges Vulnerability - CVE-2017-15548	VMware vSphere Data Protection is prone to an escalation of privielges vulnerability which enables a remote unauthenticated attacker to bypass application authentication and gain unauthorized root access to affected systems.	Version(s): <= 5.*, 6.1 - 6.1.5, 6.0 - 6.0.6	Published - January 02, 2018 CVE-2017-15548 CVSS - 9.8 Vendor's Advisory - http://www.securityfocus.com/bid/102352 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-15548 https://www.vmware.com/us/security/advisories/VMSA-2018-0001.html
Vmware vSphere Data Protection Remote Arbitrary File Upload Vulnerability - CVE-2017-15549	Vmware vSphere Data Protection (VDP) is prone to a remote arbitrary file upload vulnerability. A remote authenticated attacker could exploiut the flaw to upload crafted files to the server file system.	Version(s): <= 5.*, 6.1 - 6.1.5, 6.0 - 6.0.6	Published - January 02, 2018 CVE-2017-15549 CVSS - 6.5 Vendor's Advisory - http://www.securityfocus.com/bid/102363 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-15549 https://www.vmware.com/us/security/advisories/VMSA-2018-0001.html
[MS18-JAN] Microsoft Windows Elevation of Privilege Vulnerability in Subsystem for Linux - CVE-2018-0743	Microsoft Windows 10 and Windows Server, version 1709 (Server Core Installation) are vulnerable to elevation of privileges in the Windows Subsystem for Linux. A local authenticated attacker could gain privileges on the affected system via a crafted application.	Version(s): <= 1709 Datacenter x6, 1709 Standard x64	Published - January 03, 2018 CVE-2018-0743 CVSS - 7.0 Vendor's Advisory - https://portal.msrc.microsoft.com/en-us/security-guidance http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0743
[MS18-JAN] Microsoft Scripting Engine Memory Corruption Vulnerability - CVE-2018-0762	Internet Explorer 9 on Windows Server 2008, Internet Explorer 10 on Windows Server 2012, Internet Explorer 11 on Windows 7, Windows 8.1, Windows 10, Windows Server 2008 R2 , Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, and ChakreCore before 1.7.6 are prone to a remote code execution vulnerability due to the way the scripting engine handles objects in memory.	Version(s): < 1.7.6	Published - January 03, 2018 CVE-2018-0762 CVSS - 7.5 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-11890 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11890
[cisco-sa-20180104-cpusidechannel] Cisco Information Disclosure Vulnerability in CPU Microcode (Meltdown)- CVE-2017-5754	A flaw in the implementation of speculative execution of instructions in various microprocessors (AKA Meltdown attack), as used in multiple Cisco products, could allow an unprivileged local attacker to load rogue data cache thus crossing the syscall boundary and reading privileged memory by conducting targeted cache side-channel attacks. This issue affects multiple Cisco Unified Computing System (UCS) based systems: UCS B-Series M2 through M5 Blade Servers, UCS C-Series M2 through M5 Rack Servers, UCS B260 M4 Blade Server as well as UCS B460 M4 Blade and Rack Servers.	Version(s): <= 3.2(1d), 3.2(1d)C, 2.2(0.6)B	Published - January 03, 2018 CVE-2017-5754 CVSS - 6.5 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5754 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-5754
Red Hat JBoss Enterprise Application Platform 7.0 Local Privilege Escalation - CVE-2017-12189	Red Hat JBoss Enterprise Application Platform 7.4 is prone to local privilege escalation due to jboss init unsafe file handling.	Version(s): <= 7.0 EL7, 7.0 EL6	Published - January 03, 2018 CVE-2017-12189 CVSS - 8.4 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-12189 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-12189
Linux Kernel Remote Use-After-Free and Memory Corruption Vulnerability - CVE-2017-18017	The tcpmss_mangle_packet function in net/netfilter/xt_TCPMSS.c in the Linux kernel before 4.11, and 4.9.x before 4.9.36, allows remote attackers to cause a denial of service (use-after-free and memory corruption) or possibly have unspecified other impact by leveraging the presence of xt_TCPMSS in an iptables action.	Version(s): <= 4.10 - 4.10.9, <4.9.36	Published - January 03, 2018 CVE-2017-18017 CVSS - 9.8 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-18017 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-18017
Linux Kernel <=4.14.12 Local Information Disclosure Vulnerability due to Branch Target Injection (Spectre) - CVE-2017-5715	Linux Kernel through 4.14.12 is vulnerable to information disclosure in the form of unintended memory reads. A flaw in the implementation of speculative execution of instructions in various microprocessors by Intel, AMD, ARM and other vendors could allow an unprivileged local attacker to leverage branch target injection, leading to privileged memory read by conducting targeted cache side-channel attacks. AKA Spectre attack.	Version(s): Linux Kernel <= 4.14.12, Enterprise linux Server : 7, TUS 7.4, TUS 6.6, AUS 6.2, AUS 6.4, EUS 7.4, AUS 6.6, AUS 6.5, AUS 7.4 Enterprise linux Workstation 7	Published - January 03, 2018 CVE-2017-5715 CVSS - 5.6 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5715 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-5715