Security Advisory | Volume 2017-262-1

PRODUCT	DESCRIPTION	AFFECTED VERSIONS	OTHER INFORMATION
[cisco-sa-20170907-struts2] Cisco Multiple Products Remote Code Execution in Apache Struts - CVE-2017-9805	Cisco MXE 3500 Series Media Experience Engines, Unified Contact Center Enterprise 10.5(1), 11.0(1), 11.5(1), 11.6(1), Unified Intelligent Contact Management Enterprise and Network Performance Analysis allow a remote attacker to execute arbitrary code due to an issue in Apache Struts.	Version(s): <= 10.5(1), 11.0(1), 11.5(1), 11.6(1)	Published - September 06, 2017 CVE-2017-9805 CVSS - 9.8 Vendor's Advisory - http://www.securityfocus.com/bid/100609 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-9805 http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170907-struts2
Google Android <=8.0 Remote Elevation of Privilege in Qualcomm Video Driver - CVE-2017-8277	A remote elevation of privilege vulnerability in the Qualcomm Video driver in Android 8.0 and earlier before 2017-09-05 could enable a local malicious application to execute arbitrary code on the affected system with higher privileges. Android ID: A-62378788. References: QC-CR#2009047.	Version(s): <=8.0	Published - September 06, 2017 CVE-2017-8277 CVSS - 9.8 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-8277 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8277
[cisco-sa-20170906-isr] Cisco IR800 Integrated Services Router Local Code Execution Vulnerability	A vulnerability in the ROM Monitor (ROMMON) code of Cisco IR800 Integrated Services Router Software could allow an unauthenticated, local attacker to boot an unsigned Hypervisor on an affected device and compromise the integrity of the system. The vulnerability is due to insufficient sanitization of user input. An attacker who can access an affected router via the console could exploit this vulnerability by entering ROMMON mode and modifying ROMMON variables. A successful exploit could allow the attacker to execute arbitrary code and install a malicious version of Hypervisor firmware on an affected device. Cisco Bug IDs: CSCvb44027.	Version(s): = 15.6(1)T	Published - September 06, 2017 CVE-2017-12223 CVSS - 8.4 Vendor's Advisory - http://www.securityfocus.com/bid/100689 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-12223 http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170906-isr
MIT Kerberos 5 Remote Unspecified Impact due to Double Free Vulnerability	Double free vulnerability in MIT Kerberos 5 (aka krb5) allows attackers to have unspecified impact via vectors involving automatic deletion of security contexts on error.	Version(s): <= *	Published - September 07, 2017 CVE-2017-11462 CVSS - 9.8 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-11462 http://www.tenable.com/plugins/index.php?view=single&id=103098 https://bugzilla.redhat.com/show_bug.cgi?id=1488873 http://krbdev.mit.edu/rt/Ticket/Display.html?id=8598
Linux Kernel Local Race Condition Vulnerability - CVE-2017-12146	The driver_override implementation in drivers/base/platform.c in the Linux kernel before 4.12.1 allows local users to gain privileges by leveraging a race condition between a read operation and a store operation that involve different overrides.	Version(s): <= 4.12.1	Published - September 08, 2017 CVE-2017-12146 CVSS - 7.8 Vendor's Advisory - http://www.securityfocus.com/bid/100651 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-12146 https://source.android.com/security/bulletin/2017-09-01
[MS17-SEP] Microsoft Windows DHCP Server Remote Code Execution Vulnerability - CVE-2017-8686	The Windows Server DHCP service in Windows Server 2012 Gold and R2, and Windows Server 2016 allows an attacker to either run arbitrary code on the DHCP failover server or cause the DHCP service to become nonresponsive, due to a memory corruption vulnerability in the Windows Server DHCP service, aka "Windows DHCP Server Remote Code Execution Vulnerability".	Version(s): <= Windows Server 2012 Gold and R2, and Windows Server 2016	Published - September 12, 2017 CVE-2017-8686 CVSS - 9.8 Vendor's Advisory - http://www.securityfocus.com/bid/100730 https://qualysguard.qualys.com/fo/common/vuln_info.php?allow_modify=1&id=91408 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-8686
Linux kernel 3.3-rc1 - 4.13.1 Remote Code Execution due to a Flaw in Native Bluetooth Stack "BlueBorne" Vulnerability	The native Bluetooth stack in the Linux Kernel (BlueZ), starting at the Linux kernel version 3.3-rc1 and up to and including 4.13.1, are vulnerable to a stack overflow vulnerability in the processing of L2CAP configuration responses resulting in remote code execution in kernel space.	Version(s): <= 3.3\-rc1 - 4.13.1	Published - September 12, 2017 CVE-2017-1000251 CVSS - 9.8 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-1000251 https://access.redhat.com/security/vulnerabilities/blueborne https://www.armis.com/blueborne
[cisco-sa-20170913-cmsturn] Cisco Meeting Server Remote Restrictions Bypass or Information Disclosure in TURN	A vulnerability in the Traversal Using Relay NAT (TURN) server included with Cisco Meeting Server (CMS) could allow an authenticated, remote attacker to gain unauthenticated or unauthorized access to components of or sensitive information in an affected system. The vulnerability is due to an incorrect default configuration of the TURN server, which could expose internal interfaces and ports on the external interface of an affected system. An attacker could exploit this vulnerability by using a TURN server to perform an unauthorized connection to a Call Bridge, a Web Bridge, or a database cluster in an affected system, depending on the deployment model and CMS services in use. A successful exploit could allow the attacker to gain unauthenticated access to a Call Bridge or database cluster in an affected system or gain unauthorized access to sensitive meeting information in an affected system. To exploit this vulnerability, the attacker must have valid credentials for the TURN server of the affected system. This vulnerability affects Cisco Meeting Server (CMS) deployments that are running a CMS Software release prior to Release 2.0.16, 2.1.11, or 2.2.6. Cisco Bug IDs: CSCvf51127.	Version(s): <= 2.1 - 2.1.10, 2.2 - 2.2.5, <2.0.16	Published - September 13, 2017 CVE-2017-12249 CVSS - 9.1 Vendor's Advisory - http://www.securityfocus.com/bid/100821 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-12249 http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170913-cmsturn
VMWare ESXi, Workstation and Fusion Remote Code Execution Vulnerability in SVGA Device	VMWare ESXi 6.5 before patch ESXi650-201707101-SG , Workstation and Workstation Pro versions 12.x before 12.5.7, Fusion and Fusion Pro versions 8.x before 8.5.8 are prone to a remote code execution vulnerability due to an out-of-bounds write in the SVGA device.	Version(s): <= 12.0.0 - 12.5.6, 8.0.0 - 8.5.7, 6.5	Published - September 14, 2017 CVE-2017-4924 CVSS - 9.8 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-4924 https://blogs.vmware.com/security/2017/09/new-vmware-security-advisory-vmsa-2017-0015.html http://kb.vmware.com/kb/2149933
Apache Tomcat 7.0.0 - 7.0.79 on Windows Remote Code Execution Vulnerability	When running Apache Tomcat 7.0.0 through 7.0.79 on Windows with HTTP PUTs enabled (e.g. via setting the readonly initialisation parameter of the Default to false) it was possible to upload a JSP file to the server via a specially crafted request. This JSP could then be requested and any code it contained would be executed by the server.	Version(s): <= 7.0.0 - 7.0.79	Published - September 19, 2017 CVE-2017-12615 CVSS - 9.8 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-12615 https://lists.apache.org/thread.html/8fcb1e2d5895413abcf266f011b9918ae03e0b7daceb118ffbf23f8c@%3Cannounce.tomcat.apache.org%3E