Security Advisory | Volume 2018-037

PRODUCT	DESCRIPTION	AFFECTED VERSIONS	OTHER INFORMATION
VMWare vRealize Automation, vSphere Integrated Containers on Linux Remote Code Execution related to Xenon - CVE-2017-4947	VMWare vRealize Automation 7.2 before patch KB52320 and 7.3 before patches KB52326 and KB52316, and vSphere Integrated Containers before version 1.3.0 runnng on Linux are prone to remote code execution due to a deserialization vulnerability via Xenon.	Version(s): <= 7.2, 7.3	Published - January 26, 2018 CVE-2017-4947 CVSS - 9.8 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-4947 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-4947 https://www.vmware.com/il/security/advisories/VMSA-2018-0006.html
VMWare AirWatch Console CSRF Vulnerability - CVE-2017-4951	VMWare AirWatch Console versions 9.2.x before 9.2.2 and 9.1.x before 9.1.5 are prone to a cross-site request forgery vulnerability when accessing the App Catalog. A remote attacker could exploit the flaw by enticing users to install a crafted application.	Version(s): <= 9.2.0, 9.2.1, 9.1.0 - 9.1.4	Published - January 26, 2018 CVE-2017-4951 CVSS - 9.6 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-4951 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-4951 https://www.vmware.com/il/security/advisories/VMSA-2018-0006.html
Electrum <=2.9.4 and 3.x - 3.0.5 Python Console Remote Code Execution Vulnerability - CVE-2018-6353	The Python console in Electrum through 2.9.4 and 3.x through 3.0.5 supports arbitrary Python code without considering (1) social-engineering attacks in which a user pastes code that they do not understand and (2) code pasted by a physically proximate attacker at an unattended workstation, which makes it easier for attackers to steal Bitcoin via hook code that runs at a later time when the wallet password has been entered, a different vulnerability than CVE-2018-1000022.	Version(s): <= 2.9.4, 3.0 - 3.0.5	Published - January 27, 2018 CVE-2018-6353 CVSS - 9.8 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-6353 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-6353 https://github.com/spesmilo/electrum/issues/3678
acurax-social-media-widget Plugin for WordPress Remote CSRF Vulnerability - CVE-2018-6357	The acx_asmw_saveorder_callback function in function.php in the acurax-social-media-widget plugin before 3.2.6 for WordPress has CSRF via the recordsArray parameter to wp-admin/admin-ajax.php, with resultant social_widget_icon_array_order XSS.	Version(s): = 3.2.6	Published - January 27, 2018 CVE-2018-6357 CVSS - 9.6 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-6357 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-6357 http://lists.openwall.net/full-disclosure/2018/01/10/8
[cisco-sa-20180129-asa1] Cisco ASA and FTD Remote DoS or Code Execution Vulnerability in VPN SSL - CVE-2018-0101	A vulnerability in the Secure Sockets Layer (SSL) VPN functionality of the Cisco Adaptive Security Appliance (ASA) Software could allow an unauthenticated, remote attacker to cause a reload of the affected system or to remotely execute code. The vulnerability is due to an attempt to double free a region of memory when the webvpn feature is enabled on the Cisco ASA device. An attacker could exploit this vulnerability by sending multiple, crafted XML packets to a webvpn-configured interface on the affected system. An exploit could allow the attacker to execute arbitrary code and obtain full control of the system, or cause a reload of the affected device. This vulnerability affects Cisco ASA Software that is running on the following Cisco products: 3000 Series Industrial Security Appliance (ISA), ASA 5500 Series Adaptive Security Appliances, ASA 5500-X Series Next-Generation Firewalls, ASA Services Module for Cisco Catalyst 6500 Series Switches and Cisco 7600 Series Routers, ASA 1000V Cloud Firewall, Adaptive Security Virtual Appliance (ASAv), Firepower 2100 Series Security Appliance, Firepower 4110 Security Appliance, Firepower 9300 ASA Security Module, Firepower Threat Defense Software (FTD).	Version(s): <= 9.5 - 9.8, 8.*, 9.9, 9.0, 9.1 - 9.4	Published - January 29, 2018 CVE-2018-0101 CVSS - 10.0 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0101 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0101 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180129-asa1
Linux Kernel <4.12.4 Remote DoS or Other Vulnerability in Drivers/input/serio/i8042.c - CVE-2017-18079	Drivers/input/serio/i8042.c in the Linux kernel before 4.12.4 allows attackers to cause a denial of service (NULL pointer dereference and system crash) or possibly have unspecified other impact because the port->exists value can change after it is validated.	Version(s): <= 4.12.4	Published - January 29, 2018 CVE-2017-18079 CVSS - 9.8 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-18079 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-18079 http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=340d394a789518018f834ff70f7534fc463d3226
IBM WebSphere Application Server Remote Escalation of Privileges Vulnerability - CVE-2017-1731	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 could provide weaker than expected security when using the Administrative Console. An authenticated remote attacker could exploit this vulnerability to possibly gain elevated privileges.	Version(s): <= 7.0 - 7.0.0.43, 8.5 - 8.5.5.13, 9.0 - 9.0.0.6, 8.0 - 8.0.0.14	Published - January 30, 2018 CVE-2017-1731 CVSS - 9.8 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-1731 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-1731 http://www-01.ibm.com/support/docview.wss?uid=swg22012345&myns=swgws&mynp=OCSSEQTP&mync=R&cm_sp=swgws-_-OCSSEQTP-_-R
Apache Tomcat Native Connector Remote Unspecified Vulnerability Related to OCSP check	Apache Tomcat Native Connector 1.1.23 through 1.1.34 and 1.2.0 before 1.2.16 incorrectly verify client certificates. This issue exists due to a flaw in the parsing of AIA-Extension field, specifically when using the OCSP check. A remote attacker could exploit this issue to cause an unspecified impact on the affected system.	Version(s): <= 1.2.0 - 1.2.15, 1.1.23 - 1.1.34	Published - January 31, 2018 CVE-2017-15698 CVSS - 9.8 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-15698 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-15698 http://tomcat.apache.org/security-native.html
Citrix NetScaler VPX <=NS12.0 53.13.nc SSRF Vulnerability via webpp Account - CVE-2018-6186	Citrix NetScaler VPX through NS12.0 53.13.nc allows an SSRF attack via the /rapi/read_url URI by an authenticated attacker who has a webapp account. The attacker can gain access to the nsroot account, and execute remote commands with root privileges.	Version(s): <= 12.0 build53.13.nc	Published - February 01, 2018 CVE-2018-6186 CVSS - 9.8 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-6186 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-6186 https://gist.github.com/buxu/04ce809eb8b32ef57e232eab5e61f023
SyncBreeze Enterprise Remote Code Execution Vulnerability - CVE-2018-6537	A buffer overflow vulnerability in the control protocol of Flexense SyncBreeze Enterprise v10.4.18 allows remote attackers to execute arbitrary code by sending a crafted packet to TCP port 9121.	Version(s): <= 10.4.18	Published - February 02, 2018 CVE-2018-6537 CVSS - 9.8 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-6537 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-6537 https://www.exploit-db.com/exploits/43936/