Security Advisory | Volume 2017-311-1

PRODUCT	DESCRIPTION	AFFECTED VERSIONS	OTHER INFORMATION
Kerberos 5 Remote Buffer Overflow Vulnerability in get_matching_data() Function - CVE-2017-15088	MIT Kerberos 5 is prone to buffer overflow vulnerability. Get_matching_data() function does not properly handle situations where both CA cert and user cert have a long subject that affects krb5 with certauth plugin. Successful exploitation of this vulnerability will require a validated certificate with long subject and issuer as well as "pkinit_cert_match" string attribute in the data base.	Version(s): <= 1.15.2	Published - October 27, 2017 CVE-2017-15088 CVSS - 9.8 Vendor's Advisory - http://www.securityfocus.com/bid/101594 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-15088 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-15088
[alert-cve-2017-10151-4016513-Fusion-Middleware] Oracle Identity Manager Remote Code Execution Vulnerability in Default Account - CVE-2017-10151	Oracle Identity Manager versions 11.1.1.7, 11.1.1.9, 11.1.2.1.0, 11.1.2.2.0, 11.1.2.3.0, and 12.2.1.3.0 is prone to a remote code execution vulnerability in Default Account. An unauthenticated remote attacker could exploit this issue to execute arbitrary code on the affected system.	Version(s): <= 11.1.1.7, 11.1.1.9, 11.1.2.1.0, 11.1.2.2.0, 11.1.2.3.0, 12.2.1.3.0	Published - October 27, 2017 CVE-2017-10151 CVSS - 10.0 Vendor's Advisory - http://www.oracle.com/technetwork/topics/security/alert-cve.html http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-10151
Apple MacOS X <10.13.1 Remote Authentication Requirements Bypass Vulnerability in Apache - CVE-2017-3167	In Apache httpd, as used in Apple MacOS X before 10.13.1, the use of the ap_get_basic_auth_pw() by third-party modules outside of the authentication phase may lead to authentication requirements being bypassed. This issue was previously published by Apple as fixed in MacOS X 10.13 (HT208144).	Version(s): <= 10.13.1	Published - October 27, 2017 CVE-2017-3167 CVSS - 9.8 Vendor's Advisory - http://www.securityfocus.com/bid/99135 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-3167 https://support.apple.com/en-il/HT208221
Docker Moby <=17.03.2-ce Remote Unspecified Vulnerability in oci/defaults.go	The DefaultLinuxSpec function in oci/defaults.go in Docker Moby through 17.03.2-ce does not block /proc/scsi pathnames, which allows attackers to trigger data loss (when certain older Linux kernels are used) by leveraging Docker container access to write a "scsi remove-single-device" line to /proc/scsi/scsi, aka SCSI MICDROP.	Version(s): <= 17.03.2-ce	Published - November 04, 2017 CVE-2017-16539 CVSS - 9.8 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-16539 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-16539
Google Android 5.0.2, 5.1.1 Remote Code Execution Vulnerability in OpenSSL EVP_EncodeUpdate() - CVE-2016-2105	Google Android versions 5.0.2 and 5.1.1 are vulnerable to remote code execution via integer overflow in OpenSSL's EVP_EncodeUpdate function. AKA Android internal bug 63710022. NOTE: The 2017-11-05 patch level applies for Pixel and Nexus devices only.	Version(s): <= 5.0.2, 5.1.1	Published - November 06, 2017 CVE-2016-2105 CVSS - 9.8 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2105 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-2105
Apache Storm Remote Arbitrary File Read Vulnerability - CVE-2014-0115	Directory traversal vulnerability in the log viewer in Apache Storm 0.9.0.1 allows remote attackers to read arbitrary files via a .. (dot dot) in the file parameter to log.	Version(s): <= 0.9.0.1	Published - October 30, 2017 CVE-2014-0115 CVSS - 5.3 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0115 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-0115
Linux Kernel Local DoS or Unspecified Vulnerability - CVE-2017-12193	An incorrect node-splitting in the 'assoc_array' implementation that occurs in the 'assoc_array_apply_edit()' function in Linux Kernel 3.13 allows local users to cause a denial of service or possibly have unspecified other impact due to a null pointer dereference error.	Version(s): <= 3.13	Published - November 02, 2017 CVE-2017-12193 CVSS - 7.8 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-12193 http://www.securityfocus.com/bid/101678 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-12193
Brother Debut Embedded HTTPD Server Remote DoS Vulnerability - CVE-2017-16249	Debut Embedded HTTPD Server as used in multiple Brother printers is prone to remote denial-of-service vulnerability. A remote unauthenticated attacker could exploit this weakness by sending a malicious HTTP POST request causing the device to hang.	Version(s): <= 1.2	Published - November 02, 2017 CVE-2017-16249 CVSS - 7.5 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-16249 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-16249
BadRabbit – Ransomware	If you're using traditional signature-based security, you are at risk. BadRabbit is similar to Petya/NotPetya. However, unlike NotPetya, it doesn't use the EternalBlue exploit. The initial executable pretends to be an Adobe Flash update. It relies purely on social engineering, encouraging user interaction. Malwarebytes customers are protected against this specific ransomware variant. Be cautious with the below websites Payment site: http://caforssztxqzf2nm[.]onion InjectURL: http://185.149.120[.]3/scholargoogle/ Distribution URL: hxxp://1dnscontrol[.]com/flash_install.php	Version(s): <= *	Vendor's Advisory - http://www.zdnet.com/article/bad-rabbit-ten-things-you-need-to-know-about-the-latest-ransomware-outbreak https://www.welivesecurity.com/2017/10/24/bad-rabbit-not-petya-back