Security Advisory | Volume 2017-248

PRODUCT	DESCRIPTION	AFFECTED VERSIONS	OTHER INFORMATION
ImageMagick <6.9.9-0 and 7.0 - 7.0.6-0 Remote Out-of-Bounds Read Vulnerability - CVE-2017-13139	In ImageMagick before 6.9.9-0 and 7.x before 7.0.6-1, the ReadOneMNGImage function in coders/png.c has an out-of-bounds read with the MNG CLIP chunk.	Version(s): <= 6.9.9\-0, 7.0.6\-0	Published - August 23, 2017 CVE-2017-13139 CVSS - 9.8 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-13139 https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=870109
Google Android <=8.0 Remote Elevation of Privilege in Qualcomm Camera Driver - CVE-2017-8247	A remote elevation of privilege vulnerability in the Qualcomm Camera 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-62378684. References: QC-CR#2023513.	Version(s): <=8.0	Published - September 06, 2017 CVE-2017-8247 CVSS - 9.8 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-8247 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8247
Linux kernel Remore DoS or Code Execution Vulnerability in net/core/flow_dissector.c - CVE-2017-13715	The __skb_flow_dissect function in net/core/flow_dissector.c in the Linux kernel before 4.3 does not ensure that n_proto, ip_proto, and thoff are initialized, which allows remote attackers to cause a denial of service (system crash) or possibly execute arbitrary code via a single crafted MPLS packet.	Version(s): <= 4.3	Published - August 28, 2017 CVE-2017-13715 CVSS - 9.8 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-13715 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-13715 http://www.securityfocus.com/bid/100517
OpenSSL Out-of-Bounds Read Vulnerability	While parsing an IPAddressFamily extension in an X.509 certificate, it is possible to do a one-byte overread. This would result in an incorrect text display of the certificate. This bug has been present since 2006 and is present in all versions of OpenSSL since then. Currently 1.1.0f and earlier.	Version(s): <= 1.1.0f	Published - August 28, 2017 CVE-2017-3735 CVSS - 9.8 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3735 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-3735 http://www.securityfocus.com/bid/100515
Red Hat Jboss Enterprise Application Platform 5.0 Remote Code Execution via Crafted Serialized Data - CVE-2017-12149	Red Hat Jboss Enterprise Application Platform 5.0 doFilter method in the ReadOnlyAccessFilter of the HTTP Invoker does not properly restrict the classes for which it performs deserialization, making it prone to a remote code execution vulnerability. A remote attacker could send maliciously crafted serialized data to exploit this issue and execute arbitrary code in the context of the affected application.	Version(s): <= 5.0	Published - August 29, 2017 CVE-2017-12149 CVSS - 9.8 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-12149 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-12149 https://bugzilla.redhat.com/show_bug.cgi?id=1486220
OpenJPEG 2.2.0 Remote DoS or Unspecified Vulnerability - CVE-2017-14040	An invalid write access was discovered in bin/jp2/convert.c in OpenJPEG 2.2.0, triggering a crash in the tgatoimage function. The vulnerability may lead to remote denial of service or possibly unspecified other impact.	Version(s): <= 2.2.0	Published - August 30, 2017 CVE-2017-14040 CVSS - 8.8 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-14040 https://access.redhat.com/security/cve/CVE-2017-14040 http://www.securityfocus.com/bid/100553
Arris Modems NVG589 and NVG599 Multiple Vulnerabilities	Arris broadband modems NVG589 and NVG599 are prone to multiple vulnerabilities including several hard coded credentials that could enable a remote attacker to access the cshell service or device information and a command injection vulnerability.	Version(s): <= NVG599, NVG589	Published - August 31, 2017 SBV-75549 CVSS - 9.8 Vendor's Advisory - http://www.theregister.co.uk/2017/09/01/att_customers_with_arris_modems_at_risk_claim_infosec_bods/ https://www.nomotion.net/blog/sharknatto/
RubyGems Remote Security Bypass Vulnerability - CVE-2017-0899	RubyGems version 2.6.12 and earlier is vulnerable to maliciously crafted gem specifications that include terminal escape characters. Printing the gem specification would execute terminal escape sequences.	Version(s): <= 2.6.13	Published - August 31, 2017 CVE-2017-0899 CVSS - 9.8 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0899 http://www.securityfocus.com/bid/100576
McAfee LiveSafe <16.0.3 Remote Unrestricted Modification Vulnerability	A man-in-the-middle attack vulnerability in the non-certificate-based authentication mechanism in McAfee LiveSafe (MLS) versions prior to 16.0.3 allows network attackers to modify the Windows registry value associated with the McAfee update via the HTTP backend-response.	Version(s): <= 16.0.3	Published - September 01, 2017 CVE-2017-3898 CVSS - 6.5 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3898 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-3898
Linux kernel Local DoS Vulnerability - CVE-2017-14106	The tcp_disconnect function in net/ipv4/tcp.c in the Linux kernel before 4.12 allows local users to cause a denial of service (__tcp_select_window divide-by-zero error and system crash) by triggering a disconnect within a certain tcp_recvmsg code path.	Version(s): <= 4.12	Published - September 01, 2017 CVE-2017-14106 CVSS - 6.2 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-14106 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-14106
CVE-2017-11216 Detail	Adobe Acrobat Reader 2017.009.20058 and earlier, 2017.008.30051 and earlier, 2015.006.30306 and earlier, and 11.0.20 and earlier has an exploitable memory corruption vulnerability in the image conversion engine when processing Enhanced Metafile Format (EMF) data related to bitmap transformations. Successful exploitation could lead to arbitrary code execution.	Version(s): <= 2017.009.20058, 2017.008.30051, 2015.006.30306, 11.0.20.	Published - August 13, 2017 CVE-2017-11216 CVSS - 8.8 Vendor's Advisory - https://nvd.nist.gov/vuln/detail/CVE-2017-11216#vulnDescriptionTitle