PRODUCT	DESCRIPTION	AFFECTED VERSIONS	OTHER INFORMATION
PostgreSQL Weak Encryption Vulnerability - CVE-2017-7546	PostgreSQL versions before 9.2.22, 9.3.18, 9.4.13, 9.5.8 and 9.6.4 are vulnerable to incorrect authentication flaw allowing remote attackers to gain access to database accounts with an empty password.	Version(s): <=9.2.22, 9.3.0 - 9.3.17, 9.4.0 - 9.4.12, 9.5.0 - 9.5.7, 9.6.0 - 9.6.3.	Published - August 11, 2017 CVE-2017-7546 CVSS - 9.8 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7546 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-7546
Apache Subversion Remote Command Execution Vulnerability - CVE-2017-9800	A maliciously constructed svn+ssh:// URL would cause Subversion clients before 1.8.19, 1.9.x before 1.9.7, and 1.10.0.x through 1.10.0-alpha3 to run an arbitrary shell command. Such a URL could be generated by a malicious server, by a malicious user committing to a honest server (to attack another user of that server's repositories), or by a proxy server. The vulnerability affects all clients, including those that use file://, http://, and plain (untunneled) svn://.	Version(s): <= 1.10.0 - 1.10.0\-alpha3, 1.9.0 - 1.9.6, 1.0.0 - 1.8.18.	Published - August 11, 2017 CVE-2017-9800 CVSS - 9.9 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-9800 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-9800 https://bugzilla.redhat.com/show_bug.cgi?id=1479686 https://subversion.apache.org/security/CVE-2017-9800-advisory.txt
Xen 4.5 - 4.9 Remote Unspecified Vulnerability due to Improper Handling of the Grant Frame	Xen maintains the _GTF_{read,writ}ing bits as appropriate, to inform the guest that a grant is in use. A guest is expected not to modify the grant details while it is in use, whereas the guest is free to modify/reuse the grant entry when it is not in use. Under some circumstances, Xen will clear the status bits too early, incorrectly informing the guest that the grant is no longer in use. A guest may prematurely believe that a granted frame is safely private again, and reuse it in a way which contains sensitive information, while the domain on the far end of the grant is still using the grant. Xen 4.9, 4.8, 4.7, 4.6, and 4.5 are affected.	Version(s): <= 4.9.*, 4.5 - 4.9.	Published - August 15, 2017 CVE-2017-12855 CVSS - 9.8 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-12855 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-12855 https://bugzilla.redhat.com/show_bug.cgi?id=1481762
Xen Remote Information Disclosure, Escalation of Privileges or DoS Vulnerability - CVE-2017-12134	Xen x86 systems featuring Linux in a backend role as well as PV x86 domains featuring Xen vdb backends are prone to data stream corruption issues due to improper merge. A malicious guest can affect memory read/write processing which could result in information disclosure, privilege escalation and denial of service. The issue may only be exploited if the block device operates with enabled 'request merging'.	Version(s): <= 3.0.2 - 4.8.0.	Published - August 15,2017 CVE-2017-12134 CVSS - 9.8 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-12134 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-12134 https://access.redhat.com/security/cve/CVE-2017-12134
[MS17-AUG] Microsoft Xamarin.iOS Elevation Of Privilege Vulnerability - CVE-2017-8665	Microsoft Xamarin.iOS 10 before 10.12 on Mac OS systems, is prone to a local privilege escalation vulnerability in the update component, because it does not properly handle directories and binaries. An attacker who is logged on to the affected system, could exploit this issue by creating a folder which would by used by another process, thus gaining root privileges.	Version(s): <=10.11*, 10 - 10.11.	Published - August 14, 2017 CVE-2017-8665 CVSS - 7.8 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-8665 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8665 https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2017-8665
PHP 7.0 before 7.0.21, 7.1 before 7.1.7 Remote Heap Use After Free Vulnerability - CVE-2017-12934	ext/standard/var_unserializer.re in PHP 7.0.x before 7.0.21 and 7.1.x before 7.1.7 is prone to a heap use after free while unserializing untrusted data, related to the zval_get_type function in Zend/zend_types.h. Exploitation of this issue can have an unspecified impact on the integrity of PHP.	Version(s): <= 7.0 - 7.0.20, 7.1 - 7.1.6.	Published - August 17, 2017 CVE-2017-12934 CVSS - 8.8 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-12934 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-12934 https://bugs.php.net/bug.php?id=74101 http://php.net/ChangeLog-7.php
Mozilla Firefox <2.0.0.8 Remote Code Execution Vulnerability - CVE-2007-5341	Mozilla Firefox before 2.0.0.8 is prone to a remote code execution vulnerability in the Venkman script debugger.	Version(s): <= 2.0.0.8.	Published - August 18, 2017 CVE-2007-5341 CVSS - 7.8 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5341 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-5341 https://bugzilla.mozilla.org/show_bug.cgi?id=325761
Red Hat JBoss Enterprise Web Server Remote DoS in OpenSSL	Red Hat JBoss Enterprise Web Server 2.1.2 allows a remote attacker to cause a denial of service due to a flaw in OpenSSL.	Version(s): <= 2 EL6, 2 EL7, 2.1.2 EL6, 2.1.2 EL7.	Published - August 21,2017 CVE-2016-6304 CVSS - 7.5 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6304 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-6304 http://www.securityfocus.com/bid/93150