PRODUCT	DESCRIPTION	AFFECTED VERSIONS	OTHER INFORMATION
Apache Struts Remote Code Execution Vulnerability - CVE-2017-9791	Apache Struts 2.3.x is prone to a remote code execution vulnerability in the Struts Showcase app in the Struts 1 plugin due to improper sanitizing of user supplied input. A remote attacker could exploit this issue via a crafted request to execute arbitrary code in the context of the affected application.	Version(s): <=2.3 - 2.3.32	Published - July 07, 2017 CVE-2017-9791 CVSS - 9.8 Vendor's Advisory - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-9791 http://www.securityfocus.com/bid/99484
PHP Remote DoS or Code Execution via Crafted Data	A stack buffer overflow in zend_ini_do_op() in PHP before 5.6.31, 7.x before 7.0.21, and 7.1.x before 7.1.7 allow a remote attacker to cause a denial of service or execute arbitrary code via carfted data. This vulnerability was published by SecurityFocus.	Version(s): <=5.6.31, 7.0 - 7.0.20, 7.1.0 - 7.1.6	Published - July 10, 2017 SBV-73548 CVSS - 9.8 Vendor's Advisory - https://bugs.php.net/bug.php?id=74603 http://php.net/ChangeLog-5.php http://php.net/ChangeLog-7.php
PHP Remote DoS or Code Execution in finish_nested_data() Function	Heap buffer overflow in finish_nested_data() in PHP before 5.6.31, 7.x before 7.0.21, and 7.1.x before 7.1.7 allow a remote attacker to execute arbitrary code via unspecified vectors. This vulnerability was published by SecurityFocus.	Version(s): <=5.6.31, 7.0 - 7.0.20, 7.1.0 - 7.1.6	Published - July 10, 2017 SBV-73549 CVSS - 9.8 Vendor's Advisory - https://bugs.php.net/bug.php?id=74111 http://php.net/ChangeLog-5.php http://php.net/ChangeLog-7.php
PHP Remote Information Disclosure or DoS Vulnerability in phar_parse_pharfile Function - CVE-2017-11147	In PHP before 5.6.30 and 7.x before 7.0.15, the PHAR archive handler could be used by attackers supplying malicious archive files to crash the PHP interpreter or potentially disclose information due to a buffer over-read in the phar_parse_pharfile function in ext/phar/phar.c.	Version(s): <7.0.0 - 7.0.14, <5.6.30	Published - July 10,2017 CVE-2017-11147 CVSS - 9.1 Vendor's Advisory - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11147 https://bugs.php.net/bug.php?id=73773 http://openwall.com/lists/oss-security/2017/07/10/6
Linux kernel <=4.11.9 Remote DoS or Other Impact in the mq_notify Function	The mq_notify function in the Linux kernel through 4.11.9 does not set the sock pointer to NULL upon entry into the retry logic. During a user-space close of a Netlink socket, it allows attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact.	Version(s): <=4.11.9	Published - July 11, 2017 CVE-2017-11176 CVSS - 9.8 Vendor's Advisory - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11176 http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=f991af3daabaecff34684fd51fac80319d1baad1
Juniper JunOS Remote DoS and Code Execution via Crafted SNMP Packets	Juniper Junos versions 12.1X*, 12.3X*, 13.3R*, 14.1R*, 14.2R*, 15.1F*, 15.1R*, 15.1X*, 16.1R*, 16.2R*, 17.1R*, 17.2R* and 17.3R* before patched versions are prone to a denial-of-service and remote code execution vulnerability on device with SNMP enabled. A remote attacker could cause the snmpd daemon to crash and restart or execute arbitrary code by sending a crafted SNMP packet.	Version(s): <= 12.1X*, 12.3X*, 13.3R*, 14.1R*, 14.2R*, 15.1F*, 15.1R*, 15.1X*, 16.1R*, 16.2R*, 17.1R*, 17.2R* and 17.3R*	Published - July 12, 2017 CVE-2017-2345 CVSS - 9.8 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2345 https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10793 http://www.juniper.net/us/en/products-services/nos/junos/