CVE-2017-12932

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2017-12932
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-08-18 03:29:00 UTC
Updated	2018-05-04 01:29:00 UTC
Description	ext/standard/var_unserializer.re in PHP 7.0.x through 7.0.22 and 7.1.x through 7.1.8 is prone to a heap use after free while

Risk And Classification

Problem Types: CWE-416

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Php	Php	7.0.0	All	All	All
Application	Php	Php	7.0.1	All	All	All
Application	Php	Php	7.0.10	All	All	All
Application	Php	Php	7.0.11	All	All	All
Application	Php	Php	7.0.12	All	All	All
Application	Php	Php	7.0.13	All	All	All
Application	Php	Php	7.0.14	All	All	All
Application	Php	Php	7.0.15	All	All	All
Application	Php	Php	7.0.16	All	All	All
Application	Php	Php	7.0.17	All	All	All
Application	Php	Php	7.0.18	All	All	All
Application	Php	Php	7.0.19	All	All	All
Application	Php	Php	7.0.2	All	All	All
Application	Php	Php	7.0.20	All	All	All
Application	Php	Php	7.0.21	All	All	All
Application	Php	Php	7.0.22	All	All	All
Application	Php	Php	7.0.3	All	All	All

Application	Php	Php	7.0.4	All	All	All
Application	Php	Php	7.0.5	All	All	All
Application	Php	Php	7.0.6	All	All	All
Application	Php	Php	7.0.7	All	All	All
Application	Php	Php	7.0.8	All	All	All
Application	Php	Php	7.0.9	All	All	All
Application	Php	Php	7.1.0	All	All	All
Application	Php	Php	7.1.1	All	All	All
Application	Php	Php	7.1.2	All	All	All
Application	Php	Php	7.1.3	All	All	All
Application	Php	Php	7.1.4	All	All	All
Application	Php	Php	7.1.5	All	All	All
Application	Php	Php	7.1.6	All	All	All
Application	Php	Php	7.1.7	All	All	All
Application	Php	Php	7.1.8	All	All	All
Application	Php	Php	7.0.0	All	All	All
Application	Php	Php	7.0.1	All	All	All
Application	Php	Php	7.0.10	All	All	All
Application	Php	Php	7.0.11	All	All	All
Application	Php	Php	7.0.12	All	All	All
Application	Php	Php	7.0.13	All	All	All
Application	Php	Php	7.0.14	All	All	All
Application	Php	Php	7.0.15	All	All	All
Application	Php	Php	7.0.16	All	All	All
Application	Php	Php	7.0.17	All	All	All
Application	Php	Php	7.0.18	All	All	All
Application	Php	Php	7.0.19	All	All	All
Application	Php	Php	7.0.2	All	All	All
Application	Php	Php	7.0.20	All	All	All
Application	Php	Php	7.0.21	All	All	All
Application	Php	Php	7.0.22	All	All	All
Application	Php	Php	7.0.3	All	All	All
Application	Php	Php	7.0.4	All	All	All
Application	Php	Php	7.0.5	All	All	All
Application	Php	Php	7.0.6	All	All	All

Application	Php	Php	7.0.7	All	All	All
Application	Php	Php	7.0.8	All	All	All
Application	Php	Php	7.0.9	All	All	All
Application	Php	Php	7.1.0	All	All	All
Application	Php	Php	7.1.1	All	All	All
Application	Php	Php	7.1.2	All	All	All
Application	Php	Php	7.1.3	All	All	All
Application	Php	Php	7.1.4	All	All	All
Application	Php	Php	7.1.5	All	All	All
Application	Php	Php	7.1.6	All	All	All
Application	Php	Php	7.1.7	All	All	All
Application	Php	Php	7.1.8	All	All	All

References

Reference	Source	Link	Tags
Debian -- Security Information -- DSA-4080-1 php7.0	DEBIAN	www.debian.org	
PHP: Multiple vulnerabilities (GLSA 201709-21) — Gentoo security	GENTOO	security.gentoo.org	
PHP: PHP 7 ChangeLog	CONFIRM	php.net	Release Notes,
PHP 'ext/standard/var_unserializer.re' Heap Based Buffer Overflow Vulnerability	BID	www.securityfocus.com	Third Party Advi
Fixed bug #74103 and bug #75054 · php/php-src@1a23ebc · GitHub	CONFIRM	github.com	Patch, Third Par
Red Hat Customer Portal	REDHAT	access.redhat.com	
PHP :: Sec Bug #74103 :: heap-use-after-free when unserializing invalid array size	CONFIRM	bugs.php.net	Issue Tracking,
Red Hat Customer Portal	REDHAT	access.redhat.com	
September 2017 PHP Vulnerabilities in NetApp Products | NetApp Product Security	CONFIRM	security.netapp.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analy

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

710414 Gentoo Linux Hypertext Preprocessor (PHP) Multiple Vulnerabilities (GLSA 201709-21)

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following license.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report