CVE-2015-2301

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

Summary

CVE	CVE-2015-2301
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-03-30 10:59:00 UTC
Updated	2023-11-07 02:25:00 UTC
Description	Use-after-free vulnerability in the phar_rename_archive function in phar_object.c in PHP before 5.5.22 and 5.6.x before 5.6

Risk And Classification

Problem Types: CWE-416

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Apple	Mac Os X	All	All	All	All
Operating System	Canonical	Ubuntu Linux	10.04	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.10	All	All	All
Operating System	Canonical	Ubuntu Linux	10.04	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.10	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Opensuse	Opensuse	13.1	All	All	All
Operating System	Opensuse	Opensuse	13.2	All	All	All
Operating System	Opensuse	Opensuse	13.1	All	All	All
Operating System	Opensuse	Opensuse	13.2	All	All	All
Application	Php	Php	All	All	All	All
Application	Php	Php	All	All	All	All

Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Hpc Node	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Hpc Node	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Hpc Node Eus	7.1	All	All	All
Operating System	Redhat	Enterprise Linux Hpc Node Eus	7.1	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.1	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.1	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All

References

Reference	Source	L
[security-announce] SUSE-SU-2015:0868-1: important: Security update for	SUSE	lis
'[security bulletin] HPSBUX03337 SSRT102066 rev.1 - HP-UX Apache Web Server Suite running Apache Web ' - MARC	HP	m
APPLE-SA-2015-09-30-3 OS X El Capitan 10.11	APPLE	lis
openSUSE-SU-2015:0644-1: moderate: Security update for php5	SUSE	lis
208.43.231.11 Git - php-src.git/commit	CONFIRM	gi
'[security bulletin] HPSBMU03409 rev.1 - HP Matrix Operating Environment, Multiple Vulnerabilities' - MARC	HP	m
208.43.231.11 Git - php-src.git/commit		gi
USN-2535-1: PHP vulnerabilities | Ubuntu	UBUNTU	w
Red Hat Customer Portal	REDHAT	rh
Red Hat Customer Portal	REDHAT	rh
PHP 'ext/phar/phar_object.c' Double Free Denial of Service Vulnerability	BID	w
Oracle Solaris Third Party Bulletin - July 2015	CONFIRM	w
Debian -- Security Information -- DSA-3198-1 php5	DEBIAN	w
Support / Security / Advisories / / MDVSA-2015:079 | Mandriva	MANDRIVA	w
Oracle Linux Bulletin - January 2016	CONFIRM	w
PHP: Multiple vulnerabilities (GLSA 201606-10) — Gentoo security	GENTOO	se
oss-security - Re: CVE Request: PHP 5.6.6 changelog	MLIST	op
Bug 1194747 – CVE-2015-2301 php: use after free in phar_object.c	CONFIRM	bu
PHP :: Sec Bug #68901 :: use after free in phar_object.c	CONFIRM	bu
'[security bulletin] HPSBMU03380 rev.1 - HP System Management Homepage (SMH) on Linux and Windows, Mu' - MARC	HP	m

Red Hat Customer Portal	REDHAT	rh
About the security content of OS X El Capitan v10.11 - Apple Support	CONFIRM	su
PHP: PHP 5 ChangeLog	CONFIRM	pl
Red Hat Customer Portal	REDHAT	rh
PHP Memory Handling Error in phar Extension Lets Remote Users Execute Arbitrary Code - SecurityTracker	SECTRACK	w
CVE Program record	CVE.ORG	w
NVD vulnerability detail	NVD	nv

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

Free CVE JSON API cve.report/api

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