



CVE-2015-4021

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

Summary

CVE	CVE-2015-4021
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-06-09 18:59:04 UTC
Updated	2026-05-06 22:30:45 UTC
Description	The phar_parse_tarfile function in ext/phar/tar.c in PHP before 5.4.41, 5.5.x before 5.5.25, and 5.6.x before 5.6.9 does not v

Risk And Classification

Primary CVSS: v2.0 5 from nvd@nist.gov

AV:N/AC:L/Au:N/C:N/I:N/A:P

Problem Types: CWE-189 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

None

Availability

Partial

AV:N/AC:L/Au:N/C:N/I:N/A:P

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Apple	Mac Os X	All	All	All	All

Application	Php	Php	5.4.39	All	All	All
Application	Php	Php	5.5.0	All	All	All
Application	Php	Php	5.5.0	alpha1	All	All
Application	Php	Php	5.5.0	alpha2	All	All
Application	Php	Php	5.5.0	alpha3	All	All
Application	Php	Php	5.5.0	alpha4	All	All
Application	Php	Php	5.5.0	alpha5	All	All
Application	Php	Php	5.5.0	alpha6	All	All
Application	Php	Php	5.5.0	beta1	All	All
Application	Php	Php	5.5.0	beta2	All	All
Application	Php	Php	5.5.0	beta3	All	All
Application	Php	Php	5.5.0	beta4	All	All
Application	Php	Php	5.5.0	rc1	All	All
Application	Php	Php	5.5.0	rc2	All	All
Application	Php	Php	5.5.1	All	All	All
Application	Php	Php	5.5.10	All	All	All
Application	Php	Php	5.5.11	All	All	All
Application	Php	Php	5.5.12	All	All	All
Application	Php	Php	5.5.13	All	All	All
Application	Php	Php	5.5.14	All	All	All
Application	Php	Php	5.5.18	All	All	All
Application	Php	Php	5.5.19	All	All	All
Application	Php	Php	5.5.2	All	All	All
Application	Php	Php	5.5.20	All	All	All
Application	Php	Php	5.5.21	All	All	All
Application	Php	Php	5.5.22	All	All	All
Application	Php	Php	5.5.23	All	All	All
Application	Php	Php	5.5.24	All	All	All
Application	Php	Php	5.5.3	All	All	All
Application	Php	Php	5.5.4	All	All	All
Application	Php	Php	5.5.5	All	All	All
Application	Php	Php	5.5.6	All	All	All
Application	Php	Php	5.5.7	All	All	All
Application	Php	Php	5.5.8	All	All	All
Application	Php	Php	5.5.9	All	All	All
Application	Php	Php	5.6.0	alpha1	All	All

Application	Php	Php	5.6.0	alpha2	All	All
Application	Php	Php	5.6.0	alpha3	All	All
Application	Php	Php	5.6.0	alpha4	All	All
Application	Php	Php	5.6.0	alpha5	All	All
Application	Php	Php	5.6.0	beta1	All	All
Application	Php	Php	5.6.0	beta2	All	All
Application	Php	Php	5.6.0	beta3	All	All
Application	Php	Php	5.6.0	beta4	All	All
Application	Php	Php	5.6.2	All	All	All
Application	Php	Php	5.6.3	All	All	All
Application	Php	Php	5.6.4	All	All	All
Application	Php	Php	5.6.5	All	All	All
Application	Php	Php	5.6.6	All	All	All
Application	Php	Php	5.6.7	All	All	All
Application	Php	Php	5.6.8	All	All	All
Application	Php	Php	All	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	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 Eus	7.1	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 Workstation	7.0	All	All	All

Vendor Declared Affected Products						
Source	Vendor	Product	Version	Platforms		
CNA	Na	N/a	affected n/a	Not specified		

References						
Reference				Source		
Red Hat Customer Portal				af854a3a-2127-422b-91ae-364da26		
PHP: Multiple vulnerabilities (GLSA 201606-10) — Gentoo security				af854a3a-2127-422b-91ae-364da26		
Red Hat Customer Portal				af854a3a-2127-422b-91ae-364da26		
[SECURITY] Fedora 20 Update: php-5.5.25-1.fc20				af854a3a-2127-422b-91ae-364da26		
APPLE-SA-2015-08-13-2 OS X Yosemite v10.10.5 and Security Update 2015-006				af854a3a-2127-422b-91ae-364da26		

[SECURITY] Fedora 21 Update: php-5.6.9-1.fc21	af854a3a-2127-422b-91ae-364da26
About the security content of OS X Yosemite v10.10.5 and Security Update 2015-006 - Apple Support	af854a3a-2127-422b-91ae-364da26
Red Hat Customer Portal	af854a3a-2127-422b-91ae-364da26
openSUSE-SU-2015:0993-1: moderate: Security update for php5	af854a3a-2127-422b-91ae-364da26
Debian -- Security Information -- DSA-3280-1 php5	af854a3a-2127-422b-91ae-364da26
PHP PHAR 'phar_parse_tarfile()' Function Remote Memory Corruption Vulnerability	af854a3a-2127-422b-91ae-364da26
PHP :: Sec Bug #69453 :: Memory Corruption in phar_parse_tarfile when entry filename starts with null	af854a3a-2127-422b-91ae-364da26
PHP Integer Overflows Let Remote Users Execute Arbitrary Code - SecurityTracker	af854a3a-2127-422b-91ae-364da26
Oracle Linux Bulletin - January 2016	af854a3a-2127-422b-91ae-364da26
Red Hat Customer Portal	af854a3a-2127-422b-91ae-364da26
Red Hat Customer Portal	af854a3a-2127-422b-91ae-364da26
PHP: PHP 5 ChangeLog	af854a3a-2127-422b-91ae-364da26
[SECURITY] Fedora 22 Update: php-5.6.9-1.fc22	af854a3a-2127-422b-91ae-364da26
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD



No vendor comments have been submitted for this CVE.

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

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered 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](#)