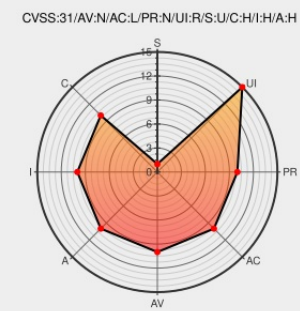
CVE-2016-4343

Published on: 05/21/2016 12:00:00 AM UTC

Last Modified on: 07/20/2022 04:31:00 PM UTC

CVE-2016-4343

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Opensuse from Opensuse contain the following vulnerability:

The phar_make_dirstream function in ext/phar/dirstream.c in PHP before 5.6.18 and 7.x before 7.0.3 mishandles zero-size ./.@LongLink files, which allows remote attackers to cause a denial of service (uninitialized pointer dereference) or possibly have unspecified other impact via a crafted TAR archive.

CVE-2016-4343 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.8 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 6.8 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
openSUSE-SU-2016:1357-1: moderate: Security update for php5	lists.opensuse.org text/html	SUSE openSUSE-SU-2016:1357
PHP: PHP 5 ChangeLog	php.net	MISC php.net/ChangeLog-5.php

	text/html	
Document Display | HPE Support Center	h20566.www2.hpe.com text/html	CONFIRM h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05320149
Document Display | HPE Support Center	h20566.www2.hpe.com text/html	CONFIRM h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05390722
Document Display | HPE Support Center	h20566.www2.hpe.com text/html	CONFIRM h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05240731
PHP: PHP 7 ChangeLog	php.net text/html	MISC php.net/ChangeLog-7.php
oss-security - [CVE Requests] PHP issues	www.openwall.com text/html	MLIST [oss-security] 20160428 [CVE Requests] PHP issues
PHP CVE-2016-4343 Uninitialized Pointer Denial of Service Vulnerability	cve.report (archive) text/html	BID 89179
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2016:2750
PHP :: Sec Bug #71331 :: Uninitialized pointer in phar_make_dirstream()	Exploit bugs.php.net text/html	CONFIRM bugs.php.net/bug.php?id=71331

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Opensuse	Opensuse	13.2	All	All	All
Application	Php	Php	All	All	All	All
Application	Php	Php	7.0.0	All	All	All
Application	Php	Php	7.0.1	All	All	All
Application	Php	Php	7.0.2	All	All	All
Application	Php	Php	7.0.0	All	All	All
Application	Php	Php	7.0.1	All	All	All
Application	Php	Php	7.0.2	All	All	All
Application	Php	Php	All	All	All	All

cpe:2.3:o:opensuse:opensuse:13.2:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:*:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:7.0.0:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:7.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:7.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:7.0.0:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:7.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:7.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→