



CVE-2016-7414

Published on: 09/17/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:06 PM UTC

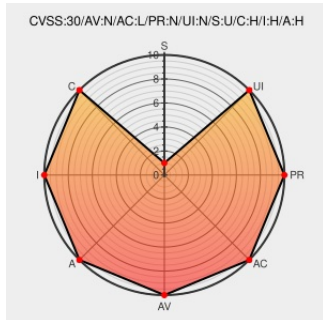
CVE-2016-7414

Source: [Mitre](#)

Source: [NIST](#)

[CVE.ORG](#)

Print: [PDF](#)



Certain versions of [Php](#) from [Php](#) contain the following vulnerability:

The ZIP signature-verification feature in PHP before 5.6.26 and 7.x before 7.0.11 does not ensure that the `uncompressed_filesize` field is large enough, which allows remote attackers to cause a denial of service (out-of-bounds memory access) or possibly have unspecified other impact via a crafted PHAR archive, related to `ext/phar/util.c` and `ext/phar/zip.c`.

CVE-2016-7414 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **CRITICAL** severity.

CVSS3 Score: **9.8 - CRITICAL**

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

CVSS2 Score: **7.5 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
PHP :: Sec Bug #72928 :: Out of bound when verify signature of zip phar in phar_parse_zipfile	Exploit Issue Tracking bugs.php.net	php CONFIRM bugs.php.net/bug.php?id=72928

	text/html	
PHP CVE-2016-7414 Heap Buffer Overflow Vulnerability	cve.report (archive) text/html	 BID 93004
PHP Multiple Memory Corruption Errors Let Remote and Local Users Execute Arbitrary Code on the Target System - SecurityTracker	www.securitytracker.com text/html	 SECTrack 1036836
[R6] SecurityCenter 5.4.1 Fixes Multiple Vulnerabilities - Security Advisory Tenable Network Security	www.tenable.com text/html	 CONFIRM www.tenable.com/security/tns-2016-19
Fix bug #72928 - Out of bound when verify signature of zip phar in ph... · php/php-src@0bfb970 · GitHub	Issue Tracking Patch github.com text/html	 CONFIRM github.com/php/php-src/commit/0bfb970f43acd1e81d11be1154805f86655f15d5?w=1
Red Hat Customer Portal	access.redhat.com text/html	 REDHAT RHSA-2018:1296
oss-security - Re: CVE assignment for PHP 5.6.26 and 7.0.11	Mailing List www.openwall.com text/html	 MLIST [oss-security] 20160915 Re: CVE assignment for PHP 5.6.26 and 7.0.11
PHP: PHP 7 ChangeLog	Release Notes www.php.net text/html	 CONFIRM www.php.net/ChangeLog-7.php
PHP: PHP 5 ChangeLog	Release Notes www.php.net text/html	 CONFIRM www.php.net/ChangeLog-5.php
PHP: Multiple vulnerabilities (GLSA 201611-22) — Gentoo security	security.gentoo.org text/html	 GENTOO GLSA-201611-22

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

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	7.0.2	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	7.0.0	All	All	All
Application	Php	Php	7.0.1	All	All	All
Application	Php	Php	7.0.10	All	All	All
Application	Php	Php	7.0.2	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	All	All	All	All
cpe:2.3:a:php:php:7.0.0:*****:						
cpe:2.3:a:php:php:7.0.1:*****:						
cpe:2.3:a:php:php:7.0.10:*****:						
cpe:2.3:a:php:php:7.0.2:*****:						
cpe:2.3:a:php:php:7.0.3:*****:						
cpe:2.3:a:php:php:7.0.4:*****:						
cpe:2.3:a:php:php:7.0.5:*****:						
cpe:2.3:a:php:php:7.0.6:*****:						
cpe:2.3:a:php:php:7.0.7:*****:						
cpe:2.3:a:php:php:7.0.8:*****:						
cpe:2.3:a:php:php:7.0.9:*****:						
cpe:2.3:a:php:php:7.0.0:*****:						
cpe:2.3:a:php:php:7.0.1:*****:						
cpe:2.3:a:php:php:7.0.10:*****:						
cpe:2.3:a:php:php:7.0.2:*****:						
cpe:2.3:a:php:php:7.0.3:*****:						
cpe:2.3:a:php:php:7.0.4:*****:						

cpe:2.3:a:php:php:7.0.5:*****:
cpe:2.3:a:php:php:7.0.6:*****:
cpe:2.3:a:php:php:7.0.7:*****:
cpe:2.3:a:php:php:7.0.8:*****:
cpe:2.3:a:php:php:7.0.9:*****:
cpe:2.3:a:php:php:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)

© [CVE.report](#) 2023   |

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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)