



# CVE-2020-7068

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2020-7068
<b>State</b>	PUBLIC
<b>Assigner</b>	security@php.net
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-09-09 18:15:00 UTC
<b>Updated</b>	2022-07-01 12:18:00 UTC
<b>Description</b>	In PHP versions 7.2.x below 7.2.33, 7.3.x below 7.3.21 and 7.4.x below 7.4.9, while processing PHAR files using phar exte

## Risk And Classification

**Problem Types:** CWE-416

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	10.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	10.0	All	All	All
Application	<a href="#">Php</a>	<a href="#">Php</a>	All	All	All	All
Application	<a href="#">Php</a>	<a href="#">Php</a>	All	All	All	All
Application	<a href="#">Tenable</a>	<a href="#">Tenable.sc</a>	All	All	All	All

## References

Reference	Source	Link	Tags
CVE-2020-7068 PHP Vulnerability in NetApp Products   NetApp Product Security	CONFIRM	<a href="#">security.netapp.com</a>	Third Pa
PHP: Denial of service (GLSA 202009-10) — Gentoo security	GENTOO	<a href="#">security.gentoo.org</a>	Third Pa
PHP :: Sec Bug #79797 :: Use of freed hash key in the phar_parse_zipfile function	CONFIRM	<a href="#">bugs.php.net</a>	Exploit,
Debian -- Security Information -- DSA-4856-1 php7.3	DEBIAN	<a href="#">www.debian.org</a>	Third Pa
[R1] Tenable.sc 5.19.0 Fixes Multiple Third-party Vulnerabilities - Security Advisory   Tenable®	CONFIRM	<a href="#">www.tenable.com</a>	
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>	canonic
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>	canonic

## Vendor Comments And Credit

Discovery Credit

**LEGACY:** grigoritchy at gmail dot com

#### Legacy QID Mappings

[159470](#) Oracle Enterprise Linux Security Update for php:7.4 (ELSA-2021-4213)

[198429](#) Ubuntu Security Notification for Hypertext Preprocessor vulnerabilities (USN-5006-1)

[239528](#) Red Hat Update for rh-php73-php (RHSA-2021:2992)

[239829](#) Red Hat Update for php:7.4 security (RHSA-2021:4213)

[690474](#) Free Berkeley Software Distribution (FreeBSD) Security Update for php72 (ee261034-b95e-4479-b947-08b0877e029f)

[752878](#) SUSE Enterprise Linux Security Update for php7 (SUSE-SU-2022:4067-1)

[752898](#) SUSE Enterprise Linux Security Update for php7 (SUSE-SU-2022:4069-1)

[752901](#) SUSE Enterprise Linux Security Update for php74 (SUSE-SU-2022:4068-1)

[940558](#) AlmaLinux Security Update for php:7.4 (ALSA-2021:4213)

[960309](#) Rocky Linux Security Update for php:7.4 (RLSA-2021:4213)

© [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](#).

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