



CVE-2020-7061

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

Summary

CVE	CVE-2020-7061
State	PUBLIC
Assigner	security@php.net
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-02-27 21:15:00 UTC
Updated	2022-05-16 19:42:00 UTC
Description	In PHP versions 7.3.x below 7.3.15 and 7.4.x below 7.4.3, while extracting PHAR files on Windows using phar extension, c

Risk And Classification

Problem Types: CWE-125

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Microsoft	Windows	-	All	All	All
Operating System	Microsoft	Windows	-	All	All	All
Application	Php	Php	All	All	All	All
Application	Php	Php	All	All	All	All
Application	Php	Php	All	All	All	All
Application	Tenable	Tenable.sc	All	All	All	All

References

Reference	Source	Link	Tags
PHP :: Sec Bug #79171 :: heap-buffer-overflow in phar_extract_file	MISC	bugs.php.net	Exploit, V
PHP: Multiple vulnerabilities (GLSA 202003-57) — Gentoo security	GENTOO	security.gentoo.org	
[R1] Tenable.sc 5.19.0 Fixes Multiple Third-party Vulnerabilities - Security Advisory Tenable®	CONFIRM	www.tenable.com	
CVE Program record	CVE.ORG	www.cve.org	canonica
NVD vulnerability detail	NVD	nvd.nist.gov	canonica

Vendor Comments And Credit

Discovery Credit

LEGACY: Reported by cmb@php.net

Legacy QID Mappings

501136 Alpine Linux Security Update for php7

© [CVE.report](https://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](https://mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://cve.mitre.org). This site includes MITRE data granted under the following [license](#).

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