



CVE-2021-21702

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

Summary

CVE	CVE-2021-21702
State	PUBLIC
Assigner	security@php.net
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-02-15 04:15:00 UTC
Updated	2021-12-10 17:58:00 UTC
Description	In PHP versions 7.3.x below 7.3.27, 7.4.x below 7.4.15 and 8.0.x below 8.0.2, when using SOAP extension to connect to a

Risk And Classification

Problem Types: CWE-476

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	10.0	All	All	All
Application	Netapp	Clustered Data Ontap	-	All	All	All
Application	Oracle	Communications Diameter Signaling Router	All	All	All	All
Application	Php	Php	All	All	All	All
Application	Php	Php	All	All	All	All

References

Reference	Source	Link	Tags
PHP :: Sec Bug #80672 :: Null Dereference in SoapClient	CONFIRM	bugs.php.net	Issue Tr
February 2021 PHP Vulnerabilities in NetApp Products NetApp Product Security	CONFIRM	security.netapp.com	
[SECURITY] [DLA 2708-1] php7.0 security update	MLIST	lists.debian.org	
Debian -- Security Information -- DSA-4856-1 php7.3	DEBIAN	www.debian.org	Third Pa
[R1] Tenable.sc 5.19.0 Fixes Multiple Third-party Vulnerabilities - Security Advisory Tenable®	CONFIRM	www.tenable.com	
Oracle Critical Patch Update Advisory - October 2021	MISC	www.oracle.com	
PHP: Multiple vulnerabilities (GLSA 202105-23) — Gentoo security	GENTOO	security.gentoo.org	

CVE Program record

CVE.ORG www.cve.org

canonic

NVD vulnerability detail

NVD nvd.nist.gov

canonic

Vendor Comments And Credit

Discovery Credit

LEGACY: Reported by jgalindo at datto dot com

Legacy QID Mappings

[150382](#) PHP Multiple Vulnerabilities (CVE-2020-7071,CVE-2021-21702)

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

[178707](#) Debian Security Update for php7.0 (DLA 2708-1)

[180436](#) Debian Security Update for php7.4 (CVE-2021-21702)

[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)

[296069](#) Oracle Solaris 11.4 Support Repository Update (SRU) 31.88.5 Missing (CPUJAN2021)

[378336](#) Zimbra Collaboration Suite (ZCS) Multiple Vulnerabilities

[38840](#) PHP Denial Of Service Vulnerability

[501142](#) Alpine Linux Security Update for php7

[501661](#) Alpine Linux Security Update for php7

[501669](#) Alpine Linux Security Update for php8

[670341](#) EulerOS Security Update for php (EulerOS-SA-2021-1883)

[710093](#) Gentoo Linux Hypertext Preprocessor Multiple vulnerabilities (GLSA 202105-23)

[750355](#) OpenSUSE Security Update for php7 (openSUSE-SU-2021:0305-1)

[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)

[901791](#) Common Base Linux Mariner (CBL-Mariner) Security Update for Hypertext Preprocessor (PHP) (7324)

[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](#)