



# CVE-2020-7069

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

## Summary

<b>CVE</b>	CVE-2020-7069
<b>State</b>	PUBLIC
<b>Assigner</b>	security@php.net
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-10-02 15:15:00 UTC
<b>Updated</b>	2023-11-07 03:25:00 UTC
<b>Description</b>	In PHP versions 7.2.x below 7.2.34, 7.3.x below 7.3.23 and 7.4.x below 7.4.11, when AES-CCM mode is used with openssl

## Risk And Classification

**Problem Types:** CWE-326

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	12.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	14.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	20.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	12.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	14.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	20.04	All	All	All
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
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	31	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	32	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	33	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	31	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	32	All	All	All

Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	33	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Clustered Data Ontap</a>	-	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Clustered Data Ontap</a>	-	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	15.1	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	15.2	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	15.1	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	15.2	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Communications Diameter Signaling Router</a>	All	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
[SECURITY] Fedora 33 Update: php-7.4.11-1.fc33 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
PHP: Multiple vulnerabilities (GLSA 202012-16) — Gentoo security	GENTOO	<a href="https://security.gentoo.org">security.gentoo.org</a>	Third Party
[SECURITY] Fedora 31 Update: php-7.3.23-1.fc31 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
[SECURITY] Fedora 32 Update: php-7.4.11-1.fc32 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
USN-4583-1: PHP vulnerabilities   Ubuntu security notices   Ubuntu	UBUNTU	<a href="https://usn.ubuntu.com">usn.ubuntu.com</a>	Third Party
Debian -- Security Information -- DSA-4856-1 php7.3	DEBIAN	<a href="https://www.debian.org">www.debian.org</a>	Third Party
[R1] Tenable.sc 5.19.0 Fixes Multiple Third-party Vulnerabilities - Security Advisory   Tenable®	CONFIRM	<a href="https://www.tenable.com">www.tenable.com</a>	
Oracle Critical Patch Update Advisory - October 2021	MISC	<a href="https://www.oracle.com">www.oracle.com</a>	
[security-announce] openSUSE-SU-2020:1703-1: important: Security update	SUSE	<a href="https://lists.opensuse.org">lists.opensuse.org</a>	Mailing List
[SECURITY] Fedora 32 Update: php-7.4.11-1.fc32 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	Third Party
[SECURITY] Fedora 31 Update: php-7.3.23-1.fc31 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	Third Party
[security-announce] openSUSE-SU-2020:1767-1: important: Security update	SUSE	<a href="https://lists.opensuse.org">lists.opensuse.org</a>	Mailing List
October 2020 PHP Vulnerabilities in NetApp Products   NetApp Product Security	CONFIRM	<a href="https://security.netapp.com">security.netapp.com</a>	Third Party
PHP :: Sec Bug #79601 :: Wrong ciphertext/tag in AES-CCM encryption for a 12 bytes IV	MISC	<a href="https://bugs.php.net">bugs.php.net</a>	Issue Tracker
[SECURITY] Fedora 33 Update: php-7.4.11-1.fc33 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	Mailing List
Oracle Critical Patch Update Advisory - April 2021	MISC	<a href="https://www.oracle.com">www.oracle.com</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical

## Vendor Comments And Credit

Discovery Credit

## LEGACY: Reported by bizxing at web dot de

### Legacy QID Mappings

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

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

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

[296070](#) Oracle Solaris 11.4 Support Repository Update (SRU) 28.82.3 Missing (CPUOCT2020)

[501140](#) Alpine Linux Security Update for php7

[501659](#) Alpine Linux Security Update for php7

[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](#)