



# CVE-2020-7064

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

## Summary

<b>CVE</b>	CVE-2020-7064
<b>State</b>	PUBLIC
<b>Assigner</b>	security@php.net
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-04-01 04:15:00 UTC
<b>Updated</b>	2022-08-29 20:04:00 UTC
<b>Description</b>	In PHP versions 7.2.x below 7.2.9, 7.3.x below 7.3.16 and 7.4.x below 7.4.4, while parsing EXIF data with exif_read_data()

## Risk And Classification

### Problem Types: CWE-125

## 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>	19.10	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>	19.10	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>	8.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	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>	8.0	All	All	All

Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	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>	15.1	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
Debian -- Security Information -- DSA-4719-1 php7.3	DEBIAN	<a href="http://www.debian.org">www.debian.org</a>	Third Pa
March 2020 PHP Vulnerabilities in NetApp Products   NetApp Product Security	CONFIRM	<a href="https://security.netapp.com">security.netapp.com</a>	Third Pa
[security-announce] openSUSE-SU-2020:0642-1: moderate: Security update f	SUSE	<a href="https://lists.opensuse.org">lists.opensuse.org</a>	Mailing L
[SECURITY] [DLA 2188-1] php5 security update	MLIST	<a href="https://lists.debian.org">lists.debian.org</a>	Mailing L
[R1] Tenable.sc 5.19.0 Fixes Multiple Third-party Vulnerabilities - Security Advisory   Tenable®	CONFIRM	<a href="http://www.tenable.com">www.tenable.com</a>	
USN-4330-2: PHP vulnerabilities   Ubuntu security notices	UBUNTU	<a href="https://usn.ubuntu.com">usn.ubuntu.com</a>	Third Pa
USN-4330-1: PHP vulnerabilities   Ubuntu security notices   Ubuntu	UBUNTU	<a href="https://usn.ubuntu.com">usn.ubuntu.com</a>	Third Pa
Debian -- Security Information -- DSA-4717-1 php7.0	DEBIAN	<a href="http://www.debian.org">www.debian.org</a>	Third Pa
PHP :: Sec Bug #79282 :: Use-of-uninitialized-value in exif	MISC	<a href="https://bugs.php.net">bugs.php.net</a>	Exploit,
Oracle Critical Patch Update Advisory - January 2021	MISC	<a href="http://www.oracle.com">www.oracle.com</a>	Third Pa
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonic
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonic

## Vendor Comments And Credit

### Discovery Credit

**LEGACY:** From <https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=19581>

## Legacy QID Mappings

[296074](#) Oracle Solaris 11.4 Support Repository Update (SRU) 22.69.4 Missing (CPUAPR2020)

[501137](#) Alpine Linux Security Update for php7

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

[940250](#) AlmaLinux Security Update for php:7.3 (ALSA-2020:3662)

[960421](#) Rocky Linux Security Update for php:7.3 (RLSA-2020:3662)

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](#)**