



# CVE-2019-11034

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

## Summary

<b>CVE</b>	CVE-2019-11034
<b>State</b>	PUBLIC
<b>Assigner</b>	security@php.net
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2019-04-18 17:29:00 UTC
<b>Updated</b>	2020-10-02 13:33:00 UTC
<b>Description</b>	When processing certain files, PHP EXIF extension in versions 7.1.x below 7.1.28, 7.2.x below 7.2.17 and 7.3.x below 7.3.4

## 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>	18.10	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	19.04	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>	18.10	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	19.04	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>	8.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Storage Automation Store</a>	-	All	All	All

Application	Netapp	Storage Automation Store	-	All	All	All
Operating System	Opensuse	Leap	15.0	All	All	All
Operating System	Opensuse	Leap	15.1	All	All	All
Operating System	Opensuse	Leap	42.3	All	All	All
Operating System	Opensuse	Leap	15.0	All	All	All
Operating System	Opensuse	Leap	15.1	All	All	All
Operating System	Opensuse	Leap	42.3	All	All	All
Application	Php	Php	All	All	All	All
Application	Php	Php	All	All	All	All
Application	Redhat	Software Collections	1.0	All	All	All
Application	Redhat	Software Collections	1.0	All	All	All

## References

Reference	Source	Link	Tags
Red Hat Customer Portal	REDHAT	<a href="https://access.redhat.com">access.redhat.com</a>	Third Party Advisory
<a href="https://support.f5.com/csp/article/K44590877">support.f5.com/csp/article/K44590877</a>	CONFIRM	<a href="https://support.f5.com">support.f5.com</a>	Third Party Advisory
USN-3953-2: PHP vulnerabilities   Ubuntu security notices	UBUNTU	<a href="https://usn.ubuntu.com">usn.ubuntu.com</a>	Third Party Advisory
USN-3953-1: PHP vulnerabilities   Ubuntu security notices   Ubuntu	UBUNTU	<a href="https://usn.ubuntu.com">usn.ubuntu.com</a>	Third Party Advisory
PHP :: Sec Bug #77753 :: Heap-buffer-overflow in php_ifd_get32s	MISC	<a href="https://bugs.php.net">bugs.php.net</a>	Patch, Vendor Advisory
April 2019 PHP Vulnerabilities in NetApp Products   NetApp Product Security	CONFIRM	<a href="https://security.netapp.com">security.netapp.com</a>	Third Party Advisory
[security-announce] openSUSE-SU-2019:1503-1: moderate: Security update f	SUSE	<a href="https://lists.opensuse.org">lists.opensuse.org</a>	Mailing List, Third Party
[security-announce] openSUSE-SU-2019:1572-1: moderate: Security update f	SUSE	<a href="https://lists.opensuse.org">lists.opensuse.org</a>	Mailing List, Third Party
[SECURITY] [DLA 1803-1] php5 security update	MLIST	<a href="https://lists.debian.org">lists.debian.org</a>	Mailing List, Third Party
Debian -- Security Information -- DSA-4529-1 php7.0	DEBIAN	<a href="https://www.debian.org">www.debian.org</a>	Third Party Advisory
[security-announce] openSUSE-SU-2019:1501-1: moderate: Security update f	SUSE	<a href="https://lists.opensuse.org">lists.opensuse.org</a>	Mailing List, Third Party
Bugtraq: [SECURITY] [DSA 4529-1] php7.0 security update	BUGTRAQ	<a href="https://seclists.org">seclists.org</a>	Mailing List, Third Party
[security-announce] openSUSE-SU-2019:1573-1: moderate: Security update f	SUSE	<a href="https://lists.opensuse.org">lists.opensuse.org</a>	Mailing List, Third Party
Red Hat Customer Portal	REDHAT	<a href="https://access.redhat.com">access.redhat.com</a>	Third Party Advisory
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, analysis

## Vendor Comments And Credit

Discovery Credit

**LEGACY:** Found by OSS-Fuzz in <https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=13723>

## Legacy QID Mappings

159670 Oracle Enterprise Linux Security Update for php:7.2 (ELSA-2020-1624)

296079 Oracle Solaris 11.4 Support Repository Update (SRU) 15.5.0 Missing (CPUOCT2019)

501128 Alpine Linux Security Update for php7

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

940404 AlmaLinux Security Update for php:7.2 (ALSA-2020:1624)

960218 Rocky Linux Security Update for php:7.2 (RLSA-2020:1624)

© [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](#)