



CVE-2019-11036

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2019-11036
State	PUBLIC
Assigner	security@php.net
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-05-03 20:29:00 UTC
Updated	2023-11-07 03:02:00 UTC
Description	When processing certain files, PHP EXIF extension in versions 7.1.x below 7.1.29, 7.2.x below 7.2.18 and 7.3.x below 7.3.5

Risk And Classification

Problem Types: CWE-125

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.10	All	All	All
Operating System	Canonical	Ubuntu Linux	19.04	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.10	All	All	All
Operating System	Canonical	Ubuntu Linux	19.04	All	All	All
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All

Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Fedoraproject	Fedora	28	All	All	All
Operating System	Fedoraproject	Fedora	29	All	All	All
Operating System	Fedoraproject	Fedora	30	All	All	All
Operating System	Fedoraproject	Fedora	28	All	All	All
Operating System	Fedoraproject	Fedora	29	All	All	All
Operating System	Fedoraproject	Fedora	30	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	access.redhat.com	Thirc
[SECURITY] Fedora 30 Update: php-7.3.5-1.fc30 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	Mai
PHP 'ext/exif/exif.c' Heap Buffer Overflow Vulnerability	BID	www.securityfocus.com	Thirc
[SECURITY] Fedora 29 Update: php-7.2.18-1.fc29 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	
[security-announce] openSUSE-SU-2019:1503-1: moderate: Security update f	SUSE	lists.opensuse.org	Mai
Bugtraq: [SECURITY] [DSA 4527-1] php7.3 security update	BUGTRAQ	seclists.org	Mai
Debian -- Security Information -- DSA-4527-1 php7.3	DEBIAN	www.debian.org	Thirc
[security-announce] openSUSE-SU-2019:1572-1: moderate: Security update f	SUSE	lists.opensuse.org	Mai
[SECURITY] [DLA 1803-1] php5 security update	MLIST	lists.debian.org	Mai
CVE-2019-11036 PHP Vulnerability in NetApp Products NetApp Product Security	CONFIRM	security.netapp.com	Thirc
[SECURITY] Fedora 30 Update: php-7.3.5-1.fc30 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	
Debian -- Security Information -- DSA-4529-1 php7.0	DEBIAN	www.debian.org	Thirc
[security-announce] openSUSE-SU-2019:1501-1: moderate: Security update f	SUSE	lists.opensuse.org	Mai
Bugtraq: [SECURITY] [DSA 4529-1] php7.0 security update	BUGTRAQ	seclists.org	Mai
[SECURITY] Fedora 28 Update: php-7.2.18-1.fc28 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	

PHP :: Sec Bug #77950 :: Heap-buffer-overflow in _estrndup via exit_process_IFD_IAG	MISC	bugs.php.net	Mail
USN-3566-2: PHP vulnerabilities Ubuntu security notices	UBUNTU	usn.ubuntu.com	Thir
USN-4009-1: PHP vulnerabilities Ubuntu security notices Ubuntu	UBUNTU	usn.ubuntu.com	Thir
[SECURITY] Fedora 28 Update: php-7.2.18-1.fc28 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	Mail
[security-announce] openSUSE-SU-2019:1573-1: moderate: Security update f	SUSE	lists.opensuse.org	Mail
[SECURITY] Fedora 29 Update: php-7.2.18-1.fc29 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	Mail
Red Hat Customer Portal	REDHAT	access.redhat.com	Thir
CVE Program record	CVE.ORG	www.cve.org	cano
NVD vulnerability detail	NVD	nvd.nist.gov	cano

Vendor Comments And Credit

Discovery Credit

LEGACY: Discovered by OSS-fuzz in <https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=14050>

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)

[501129](#) 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](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://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](#).

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