CVE-2019-11034

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2019-11034
State	PUBLIC
Assigner	security@php.net
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-04-18 17:29:00 UTC
Updated	2020-10-02 13:33:00 UTC
Description	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	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	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Netapp	Storage Automation Store	-	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	access.redhat.com	Third Party Advisory
support.f5.com/csp/article/K44590877	CONFIRM	support.f5.com	Third Party Advisory
USN-3953-2: PHP vulnerabilities | Ubuntu security notices	UBUNTU	usn.ubuntu.com	Third Party Advisory
USN-3953-1: PHP vulnerabilities | Ubuntu security notices | Ubuntu	UBUNTU	usn.ubuntu.com	Third Party Advisory
PHP :: Sec Bug #77753 :: Heap-buffer-overflow in php_ifd_get32s	MISC	bugs.php.net	Patch, Vendor Advisory
April 2019 PHP Vulnerabilities in NetApp Products | NetApp Product Security	CONFIRM	security.netapp.com	Third Party Advisory
[security-announce] openSUSE-SU-2019:1503-1: moderate: Security update f	SUSE	lists.opensuse.org	Mailing List, Third Party
[security-announce] openSUSE-SU-2019:1572-1: moderate: Security update f	SUSE	lists.opensuse.org	Mailing List, Third Party
[SECURITY] [DLA 1803-1] php5 security update	MLIST	lists.debian.org	Mailing List, Third Party
Debian -- Security Information -- DSA-4529-1 php7.0	DEBIAN	www.debian.org	Third Party Advisory
[security-announce] openSUSE-SU-2019:1501-1: moderate: Security update f	SUSE	lists.opensuse.org	Mailing List, Third Party
Bugtraq: [SECURITY] [DSA 4529-1] php7.0 security update	BUGTRAQ	seclists.org	Mailing List, Third Party
[security-announce] openSUSE-SU-2019:1573-1: moderate: Security update f	SUSE	lists.opensuse.org	Mailing List, Third Party
Red Hat Customer Portal	REDHAT	access.redhat.com	Third Party Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	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)