



CVE-2019-17402

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

Summary

CVE	CVE-2019-17402
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-10-09 19:15:00 UTC
Updated	2023-01-13 16:19:00 UTC
Description	Exiv2 0.27.2 allows attackers to trigger a crash in Exiv2::getULong in types.cpp when called from Exiv2::Internal::CiffDirect

Risk And Classification

Problem Types: CWE-120

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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	19.04	All	All	All
Operating System	Canonical	Ubuntu Linux	19.10	All	All	All
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Application	Exiv2	Exiv2	0.27.2	All	All	All
Application	Exiv2	Exiv2	0.27.2	All	All	All

References

Reference	Source	Link	Tags
[SECURITY] [DLA 3265-1] exiv2 security update	MLIST	lists.debian.org	
[SECURITY] [DLA 2019-1] exiv2 security update	MLIST	lists.debian.org	
Overflow in exiv2 · Issue #1019 · Exiv2/exiv2 · GitHub	MISC	github.com	Issue Tracking, Third Party Advisory
USN-4159-1: Exiv2 vulnerability Ubuntu security notices Ubuntu	UBUNTU	usn.ubuntu.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

159213 Oracle Enterprise Linux Security Update for exiv2 (ELSA-2021-1758)
181464 Debian Security Update for exiv2 (DLA 3265-1)
239308 Red Hat Update for exiv2 (RHSA-2021:1758)
377541 Alibaba Cloud Linux Security Update for exiv2 (ALINUX2-SA-2020:0138)
500894 Alpine Linux Security Update for exiv2
504728 Alpine Linux Security Update for exiv2
670174 EulerOS Security Update for exiv2 (EulerOS-SA-2021-1674)
670294 EulerOS Security Update for exiv2 (EulerOS-SA-2021-1782)
670609 EulerOS Security Update for exiv2 (EulerOS-SA-2021-2367)
752916 SUSE Enterprise Linux Security Update for exiv2-0_26 (SUSE-SU-2022:4208-1)
752954 SUSE Enterprise Linux Security Update for exiv2 (SUSE-SU-2022:4276-1)
901628 Common Base Linux Mariner (CBL-Mariner) Security Update for exiv2 (7204)
902296 Common Base Linux Mariner (CBL-Mariner) Security Update for exiv2 (7204-1)
940006 AlmaLinux Security Update for exiv2 (ALSA-2021:1758)
960695 Rocky Linux Security Update for exiv2 (RLSA-2021:1758)

© [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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)