



# CVE-2021-29457

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

## Summary

<b>CVE</b>	CVE-2021-29457
<b>State</b>	PUBLIC
<b>Assigner</b>	security-advisories@github.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-04-19 19:15:00 UTC
<b>Updated</b>	2023-12-22 10:15:00 UTC
<b>Description</b>	Exiv2 is a command-line utility and C++ library for reading, writing, deleting, and modifying the metadata of image files. A h

## Risk And Classification

**Problem Types:** CWE-122

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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>	9.0	All	All	All
Application	<a href="#">Exiv2</a>	<a href="#">Exiv2</a>	All	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	33	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	34	All	All	All

## References

Reference	Source	Link
[SECURITY] Fedora 33 Update: exiv2-0.27.3-6.fc33 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
Heap buffer overflow in Exiv2::Jp2Image::doWriteMetadata · Advisory · Exiv2/exiv2 · GitHub	CONFIRM	<a href="https://github.com">github.com</a>
[SECURITY] Fedora 34 Update: exiv2-0.27.3-6.fc34 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
[SECURITY] Fedora 33 Update: exiv2-0.27.3-6.fc33 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
Debian -- Security Information -- DSA-4958-1 exiv2	DEBIAN	<a href="https://www.debian.org">www.debian.org</a>
Exiv2: Multiple Vulnerabilities (GLSA 202312-06) — Gentoo security		<a href="https://security.gentoo.org">security.gentoo.org</a>
[SECURITY] Fedora 34 Update: exiv2-0.27.3-6.fc34 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
[SECURITY] [DLA 2750-1] exiv2 security update	MLIST	<a href="https://lists.debian.org">lists.debian.org</a>
Fix out of buffer access in #1529 by pydera · Pull Request #1534 · Exiv2/exiv2 · GitHub	MISC	<a href="https://github.com">github.com</a>

heap-buffer-overflow write in Exiv2::Jp2Image::doWriteMetadata · Issue #1529 · Exiv2/exiv2 · GitHub	MISC	<a href="https://github.com">github.com</a>
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

<a href="#">178761</a> Debian Security Update for exiv2 (DSA 4958-1)
<a href="#">178777</a> Debian Security Update for exiv2 (DLA 2750-1)
<a href="#">179666</a> Debian Security Update for exiv2 (CVE-2021-29457)
<a href="#">198360</a> Ubuntu Security Notification for Exiv2 vulnerabilities (USN-4941-1)
<a href="#">239787</a> Red Hat Update for exiv2 security (RHSA-2021:4173)
<a href="#">281237</a> Fedora Security Update for exiv2 (FEDORA-2021-be94728b95)
<a href="#">281238</a> Fedora Security Update for exiv2 (FEDORA-2021-10d7331a31)
<a href="#">501545</a> Alpine Linux Security Update for exiv2
<a href="#">501840</a> Alpine Linux Security Update for exiv2
<a href="#">503076</a> Alpine Linux Security Update for exiv2
<a href="#">503344</a> Alpine Linux Security Update for exiv2
<a href="#">503418</a> Alpine Linux Security Update for exiv2
<a href="#">503507</a> Alpine Linux Security Update for exiv2
<a href="#">503534</a> Alpine Linux Security Update for exiv2
<a href="#">503582</a> Alpine Linux Security Update for exiv2
<a href="#">503619</a> Alpine Linux Security Update for exiv2
<a href="#">503646</a> Alpine Linux Security Update for exiv2
<a href="#">503665</a> Alpine Linux Security Update for exiv2
<a href="#">506047</a> Alpine Linux Security Update for exiv2
<a href="#">670420</a> EulerOS Security Update for exiv2 (EulerOS-SA-2021-1979)
<a href="#">670569</a> EulerOS Security Update for exiv2 (EulerOS-SA-2021-2327)
<a href="#">671050</a> EulerOS Security Update for exiv2 (EulerOS-SA-2021-2579)
<a href="#">690094</a> Free Berkeley Software Distribution (FreeBSD) Security Update for exiv2 (d49f86ab-d9c7-11eb-a200-00155d01f201)

<a href="#">710810</a> Gentoo Linux Exiv2 Multiple Vulnerabilities (GLSA 202312-06)
<a href="#">752871</a> SUSE Enterprise Linux Security Update for exiv2 (SUSE-SU-2022:4252-1)
<a href="#">752917</a> SUSE Enterprise Linux Security Update for exiv2 (SUSE-SU-2022:3889-1)
<a href="#">901949</a> Common Base Linux Mariner (CBL-Mariner) Security Update for exiv2 (7206)
<a href="#">902252</a> Common Base Linux Mariner (CBL-Mariner) Security Update for exiv2 (7206-1)
<a href="#">940296</a> AlmaLinux Security Update for exiv2 (ALSA-2021:4173)
<a href="#">960736</a> Rocky Linux Security Update for exiv2 (RLSA-2021:4173)

© [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](#)