



# CVE-2021-37615

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2021-37615
<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>	2021-08-09 20:15:00 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 n

## Risk And Classification

**Problem Types:** CWE-476

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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
Null pointer dereference in Exiv2::Internal::resolveLens0x319 · Advisory · Exiv2/exiv2 · GitHub	CONFIRM	<a href="#">github.com</a>
Check that the iterator is not end() after calling findKey by kevinbackhouse · Pull Request #1758 · Exiv2/exiv2 · GitHub	MISC	<a href="#">github.com</a>
Exiv2: Multiple Vulnerabilities (GLSA 202312-06) — Gentoo security		<a href="#">security.gentoo.org</a>
[SECURITY] Fedora 33 Update: mingw-exiv2-0.27.4-3.fc33 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="#">lists.fedoraproject.org</a>
[SECURITY] Fedora 34 Update: mingw-exiv2-0.27.4-3.fc34 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="#">lists.fedoraproject.org</a>
[SECURITY] Fedora 33 Update: mingw-exiv2-0.27.4-3.fc33 - package-announce - Fedora Mailing-Lists		<a href="#">lists.fedoraproject.org</a>
[SECURITY] Fedora 34 Update: mingw-exiv2-0.27.4-3.fc34 - package-announce - Fedora Mailing-Lists		<a href="#">lists.fedoraproject.org</a>
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

182884	Debian Security Update for exiv2 (CVE-2021-37615)
198462	Ubuntu Security Notification for Exiv2 Vulnerabilities (USN-5043-1)
281833	Fedora Security Update for mingw (FEDORA-2021-399f869889)
281834	Fedora Security Update for mingw (FEDORA-2021-cbaef8e2d5)
501842	Alpine Linux Security Update for exiv2
504732	Alpine Linux Security Update for exiv2
671041	EulerOS Security Update for exiv2 (EulerOS-SA-2021-2657)
671049	EulerOS Security Update for exiv2 (EulerOS-SA-2021-2628)
671264	EulerOS Security Update for exiv2 (EulerOS-SA-2022-1161)
710810	Gentoo Linux Exiv2 Multiple Vulnerabilities (GLSA 202312-06)
901478	Common Base Linux Mariner (CBL-Mariner) Security Update for exiv2 (7218)
902253	Common Base Linux Mariner (CBL-Mariner) Security Update for exiv2 (7218-1)

© [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](#)