



CVE-2021-34334

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2021-34334
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-08-09 18:15:00 UTC
Updated	2023-12-22 10:15:00 UTC
Description	Exiv2 is a command-line utility and C++ library for reading, writing, deleting, and modifying the metadata of image files. An i

Risk And Classification

Problem Types: CWE-835

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	10.0	All	All	All
Application	Exiv2	Exiv2	All	All	All	All
Operating System	Fedoraproject	Fedora	33	All	All	All
Operating System	Fedoraproject	Fedora	34	All	All	All

References

Reference	Source
[SECURITY] [DLA 3265-1] exiv2 security update	MLIST
Exiv2: Multiple Vulnerabilities (GLSA 202312-06) — Gentoo security	
[SECURITY] Fedora 33 Update: mingw-exiv2-0.27.4-3.fc33 - package-announce - Fedora Mailing-Lists	FEDORA
Denial of service due to integer overflow in loop counter · Advisory · Exiv2/exiv2 · GitHub	CONFIRM
[SECURITY] Fedora 34 Update: mingw-exiv2-0.27.4-3.fc34 - package-announce - Fedora Mailing-Lists	FEDORA
[SECURITY] Fedora 33 Update: mingw-exiv2-0.27.4-3.fc33 - package-announce - Fedora Mailing-Lists	
[SECURITY] Fedora 34 Update: mingw-exiv2-0.27.4-3.fc34 - package-announce - Fedora Mailing-Lists	
Extra checking to prevent loop counter from wrapping around by kevinbackhouse · Pull Request #1766 · Exiv2/exiv2 · GitHub	MISC
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

181464 Debian Security Update for exiv2 (DLA 3265-1)
183137 Debian Security Update for exiv2 (CVE-2021-34334)
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)
752871 SUSE Enterprise Linux Security Update for exiv2 (SUSE-SU-2022:4252-1)
752892 SUSE Enterprise Linux Security Update for exiv2 (SUSE-SU-2022:3892-1)
752917 SUSE Enterprise Linux Security Update for exiv2 (SUSE-SU-2022:3889-1)
901801 Common Base Linux Mariner (CBL-Mariner) Security Update for exiv2 (7215)
902340 Common Base Linux Mariner (CBL-Mariner) Security Update for exiv2 (7215-1)

© [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](#)