



CVE-2021-3482

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

Summary

CVE	CVE-2021-3482
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-04-08 23:15:00 UTC
Updated	2023-11-07 03:38:00 UTC
Description	A flaw was found in Exiv2 in versions before and including 0.27.4-RC1. Improper input validation of the rawData.size property

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Exiv2	Exiv2	0.27.4	rc1	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
Operating System	Redhat	Enterprise Linux	8.0	All	All	All

References

Reference	Source
[SECURITY] Fedora 33 Update: exiv2-0.27.3-6.fc33 - package-announce - Fedora Mailing-Lists	FEDORA
[SECURITY] Fedora 34 Update: exiv2-0.27.3-6.fc34 - package-announce - Fedora Mailing-Lists	
[SECURITY] Fedora 33 Update: exiv2-0.27.3-6.fc33 - package-announce - Fedora Mailing-Lists	
1946314 - (CVE-2021-3482) CVE-2021-3482 exiv2: heap-based buffer overflow in Jp2Image::readMetadata() in jp2image.cpp	MISC
Debian -- Security Information -- DSA-4958-1 exiv2	DEBIAN
[SECURITY] Fedora 34 Update: exiv2-0.27.3-6.fc34 - package-announce - Fedora Mailing-Lists	FEDORA
[SECURITY] [DLA 2750-1] exiv2 security update	MLIST

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[178761](#) Debian Security Update for exiv2 (DSA 4958-1)

[178777](#) Debian Security Update for exiv2 (DLA 2750-1)

[181944](#) Debian Security Update for exiv2 (CVE-2021-3482)

[198360](#) Ubuntu Security Notification for Exiv2 vulnerabilities (USN-4941-1)

[239787](#) Red Hat Update for exiv2 security (RHSA-2021:4173)

[281237](#) Fedora Security Update for exiv2 (FEDORA-2021-be94728b95)

[281238](#) Fedora Security Update for exiv2 (FEDORA-2021-10d7331a31)

[501545](#) Alpine Linux Security Update for exiv2

[501840](#) Alpine Linux Security Update for exiv2

[503076](#) Alpine Linux Security Update for exiv2

[503344](#) Alpine Linux Security Update for exiv2

[503418](#) Alpine Linux Security Update for exiv2

[503507](#) Alpine Linux Security Update for exiv2

[503534](#) Alpine Linux Security Update for exiv2

[503582](#) Alpine Linux Security Update for exiv2

[503619](#) Alpine Linux Security Update for exiv2

[503646](#) Alpine Linux Security Update for exiv2

[503665](#) Alpine Linux Security Update for exiv2

[506047](#) Alpine Linux Security Update for exiv2

[670535](#) EulerOS Security Update for exiv2 (EulerOS-SA-2021-2293)

[670569](#) EulerOS Security Update for exiv2 (EulerOS-SA-2021-2327)

[690094](#) Free Berkeley Software Distribution (FreeBSD) Security Update for exiv2 (d49f86ab-d9c7-11eb-a200-00155d01f201)

[901229](#) Common Base Linux Mariner (CBL-Mariner) Security Update for exiv2 (7217)

[902265](#) Common Base Linux Mariner (CBL-Mariner) Security Update for exiv2 (7217-1)

[940296](#) AlmaLinux Security Update for exiv2 (ALSA-2021:4173)

[960736](#) 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](#)