



CVE-2021-3405

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

Summary

CVE	CVE-2021-3405
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-02-23 20:15:00 UTC
Updated	2023-11-07 03:37:00 UTC
Description	A flaw was found in libebml before 1.4.2. A heap overflow bug exists in the implementation of EbmlString::ReadData and E

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	9.0	All	All	All
Operating System	Fedoraproject	Fedora	32	All	All	All
Operating System	Fedoraproject	Fedora	33	All	All	All
Operating System	Fedoraproject	Fedora	34	All	All	All
Operating System	Fedoraproject	Fedora	32	All	All	All
Operating System	Fedoraproject	Fedora	33	All	All	All
Application	Matroska	Libebml	All	All	All	All
Application	Matroska	Libebml	All	All	All	All

References

Reference	Source	Link
[SECURITY] Fedora 32 Update: libebml-1.4.2-1.fc32 - package-announce - Fedora Mailing-Lists		lists.fedoraproje
[SECURITY] Fedora 32 Update: libebml-1.4.2-1.fc32 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproje
[SECURITY] Fedora 33 Update: libebml-1.4.2-1.fc33 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproje
libebml: Heap buffer overflow vulnerability (GLSA 202208-21) — Gentoo security	GENTOO	security.gentoo
Ebml[Unicode]String::ReadData heap overflow bug on 32bit builds · Issue #74 · Matroska-Org/libebml · GitHub	MISC	github.com
[SECURITY] Fedora 34 Update: libebml-1.4.2-1.fc34 - package-announce - Fedora Mailing-Lists		lists.fedoraproje

[SECURITY] Fedora 33 Update: libebml-1.4.2-1.fc33 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
[SECURITY] [DLA 2629-1] libebml security update	MLIST	lists.debian.org
[SECURITY] Fedora 34 Update: libebml-1.4.2-1.fc34 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- [178535](#) Debian Security Update for libebml (DLA 2629-1)
- [180233](#) Debian Security Update for libebml (CVE-2021-3405)
- [281572](#) Fedora Security Update for libebml (FEDORA-2021-e283997bb9)
- [281573](#) Fedora Security Update for libebml (FEDORA-2021-aa78f97893)
- [281574](#) Fedora Security Update for libebml (FEDORA-2021-9a0ff8455)
- [501597](#) Alpine Linux Security Update for libebml
- [710596](#) Gentoo Linux libebml Heap buffer overflow Vulnerability (GLSA 202208-21)

© [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