



CVE-2022-36227

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2022-36227
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-11-22 02:15:00 UTC
Updated	2024-03-27 16:04:00 UTC
Description	In libarchive before 3.6.2, the software does not check for an error after calling calloc function that can return with a NULL p

Risk And Classification

Problem Types: CWE-476

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	Fedoraproject	Fedora	37	All	All	All
Application	Libarchive	Libarchive	All	All	All	All
Application	Libarchive	Libarchive	3.6.1	All	All	All
Application	Splunk	Universal Forwarder	All	All	All	All
Application	Splunk	Universal Forwarder	9.1.0	All	All	All

References

Reference	Source	Link	Ta
[SECURITY] Fedora 37 Update: libarchive-3.6.1-3.fc37 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	
There is a NULL pointer dereference vulnerability · Issue #1754 · libarchive/libarchive · GitHub	MISC	github.com	
[SECURITY] [DLA 3294-1] libarchive security update	MLIST	lists.debian.org	
[SECURITY] Fedora 37 Update: libarchive-3.6.1-3.fc37 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	
libarchive: Multiple Vulnerabilities (GLSA 202309-14) — Gentoo security	GENTOO	security.gentoo.org	
libarchive/archive_write.c at v3.0.0a · libarchive/libarchive · GitHub	MISC	github.com	
882521 – (CVE-2022-36227) app-arch/libarchive: null pointer dereference	MISC	bugs.gentoo.org	
CVE Program record	CVE.ORG	www.cve.org	ca

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[160605](#) Oracle Enterprise Linux Security Update for libarchive (ELSA-2023-2532)

[160675](#) Oracle Enterprise Linux Security Update for libarchive (ELSA-2023-3018)

[181531](#) Debian Security Update for libarchive (DLA 3294-1)

[184855](#) Debian Security Update for libarchive (CVE-2022-36227)

[241427](#) Red Hat Update for libarchive (RHSA-2023:2532)

[241480](#) Red Hat Update for libarchive (RHSA-2023:3018)

[242686](#) Red Hat Update for libarchive (RHSA-2024:0146)

[283538](#) Fedora Security Update for libarchive (FEDORA-2022-e15be0091f)

[355621](#) Amazon Linux Security Advisory for libarchive : ALAS2023-2023-246

[356413](#) Amazon Linux Security Advisory for libarchive : ALAS2-2023-2279

[356758](#) Amazon Linux Security Advisory for libarchive : ALAS2-2023-2364

[378599](#) Splunk Enterprise Third Party Package Updates for June (SVD-2023-0613)

[378883](#) Splunk Enterprise August Third Party Package Updates (SVD-2023-0808)

[502604](#) Alpine Linux Security Update for libarchive

[502605](#) Alpine Linux Security Update for libarchive

[502734](#) Alpine Linux Security Update for libarchive

[505625](#) Alpine Linux Security Update for libarchive

[672589](#) EulerOS Security Update for libarchive (EulerOS-SA-2023-1322)

[672644](#) EulerOS Security Update for libarchive (EulerOS-SA-2023-1361)

[672645](#) EulerOS Security Update for libarchive (EulerOS-SA-2023-1389)

[672696](#) EulerOS Security Update for libarchive (EulerOS-SA-2023-1426)

[672700](#) EulerOS Security Update for libarchive (EulerOS-SA-2023-1411)

[672729](#) EulerOS Security Update for libarchive (EulerOS-SA-2023-1446)

[672757](#) EulerOS Security Update for libarchive (EulerOS-SA-2023-1471)

[672800](#) EulerOS Security Update for libarchive (EulerOS-SA-2023-1451)

673083 EulerOS Security Update for libarchive (EulerOS-SA-2023-2154)
710757 Gentoo Linux libarchive Multiple Vulnerabilities (GLSA 202309-14)
752822 SUSE Enterprise Linux Security Update for libarchive (SUSE-SU-2022:4209-1)
752888 SUSE Enterprise Linux Security Update for libarchive (SUSE-SU-2022:4202-1)
752936 SUSE Enterprise Linux Security Update for libarchive (SUSE-SU-2022:4296-1)
904559 Common Base Linux Mariner (CBL-Mariner) Security Update for libarchive (11473)
904561 Common Base Linux Mariner (CBL-Mariner) Security Update for libarchive (11470)
904627 Common Base Linux Mariner (CBL-Mariner) Security Update for libarchive (11473-1)
904637 Common Base Linux Mariner (CBL-Mariner) Security Update for libarchive (11470-1)
904908 Common Base Linux Mariner (CBL-Mariner) Security Update for cmake (12316)
905079 Common Base Linux Mariner (CBL-Mariner) Security Update for cmake (12477)
941050 AlmaLinux Security Update for libarchive (ALSA-2023:2532)
941070 AlmaLinux Security Update for libarchive (ALSA-2023:3018)

© [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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)