



# CVE-2022-26280

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

## Summary

<b>CVE</b>	CVE-2022-26280
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-03-28 22:15:00 UTC
<b>Updated</b>	2023-11-07 03:44:00 UTC
<b>Description</b>	Libarchive v3.6.0 was discovered to contain an out-of-bounds read via the component zipx_lzma_alone_init.

## Risk And Classification

**Problem Types:** CWE-125

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	36	All	All	All
Application	<a href="#">Libarchive</a>	<a href="#">Libarchive</a>	3.6.0	All	All	All

## References

Reference	Source	Link
The libarchive lib exist a READ memory access Vulnerability · Issue #1672 · libarchive/libarchive · GitHub	MISC	<a href="#">github.com</a>
[SECURITY] Fedora 36 Update: libarchive-3.5.3-2.fc36 - package-announce - Fedora Mailing-Lists		<a href="#">lists.fedoraproject.or</a>
libarchive: Multiple Vulnerabilities (GLSA 202208-26) — Gentoo security	GENTOO	<a href="#">security.gentoo.org</a>
[SECURITY] Fedora 36 Update: libarchive-3.5.3-2.fc36 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="#">lists.fedoraproject.or</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

[159947](#) Oracle Enterprise Linux Security Update for libarchive (ELSA-2022-5252)

[183050](#) Debian Security Update for libarchive (CVE-2022-26280)

198737 Ubuntu Security Notification for libarchive Vulnerability (USN-5374-1)
240501 Red Hat Update for libarchive (RHSA-2022:5252)
282751 Fedora Security Update for libarchive (FEDORA-2022-bbb5ec21b2)
354321 Amazon Linux Security Advisory for libarchive : ALAS2022-2022-201
354333 Amazon Linux Security Advisory for libarchive : ALAS2022-2022-103
354576 Amazon Linux Security Advisory for libarchive : ALAS-2022-201
355173 Amazon Linux Security Advisory for libarchive : ALAS2023-2023-071
501966 Alpine Linux Security Update for libarchive
504052 Alpine Linux Security Update for libarchive
672083 EulerOS Security Update for libarchive (EulerOS-SA-2022-2293)
672125 EulerOS Security Update for libarchive (EulerOS-SA-2022-2322)
672149 EulerOS Security Update for libarchive (EulerOS-SA-2022-2416)
672165 EulerOS Security Update for libarchive (EulerOS-SA-2022-2429)
710601 Gentoo Linux libarchive Multiple Vulnerabilities (GLSA 202208-26)
752166 SUSE Enterprise Linux Security Update for libarchive (SUSE-SU-2022:1803-1)
752203 SUSE Enterprise Linux Security Update for libarchive (SUSE-SU-2022:1930-1)
901111 Common Base Linux Mariner (CBL-Mariner) Security Update for libarchive (9210)
902303 Common Base Linux Mariner (CBL-Mariner) Security Update for libarchive (9210-1)
940622 AlmaLinux Security Update for libarchive (ALSA-2022:5252)
960637 Rocky Linux Security Update for libarchive (RLSA-2022:5252)

© [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](#)**