



# Libarchive: libarchive: denial of service via malformed iso file processing

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

## Summary

<b>CVE</b>	CVE-2026-4426
<b>State</b>	PUBLISHED
<b>Assigner</b>	redhat
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-03-19 15:16:28 UTC
<b>Updated</b>	2026-05-03 21:16:11 UTC
<b>Description</b>	A flaw was found in libarchive. An Undefined Behavior vulnerability exists in the zisofs decompression logic, caused by imp

## Risk And Classification

**Primary CVSS:** v3.1 6.5 MEDIUM from secalert@redhat.com

**CVSS:** 3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

**EPSS:** 0.001240000 probability, percentile 0.311440000 (date 2026-05-03)

**Problem Types:** CWE-1335 | CWE-1335 Incorrect Bitwise Shift of Integer

Version	Source	Type	Score	Severity	Vector
3.1	secalert@redhat.com	Secondary	6.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H
3.1	CNA	CVSS	6.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

High

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

#### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Libarchive</a>	<a href="#">Libarchive</a>	-	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	10.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	6.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	8.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	9.0	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Hardened Images</a>	-	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">OpenShift Container Platform</a>	4.0	All	All	All

#### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	<a href="#">Red Hat</a>	<a href="#">Red Hat Hardened Images</a>	unaffected 3.8.7-1.hum1 * rpm	Not specified
CNA	<a href="#">Red Hat</a>	<a href="#">Red Hat Enterprise Linux 10</a>	Not specified	Not specified
CNA	<a href="#">Red Hat</a>	<a href="#">Red Hat Enterprise Linux 6</a>	Not specified	Not specified
CNA	<a href="#">Red Hat</a>	<a href="#">Red Hat Enterprise Linux 7</a>	Not specified	Not specified
CNA	<a href="#">Red Hat</a>	<a href="#">Red Hat Enterprise Linux 8</a>	Not specified	Not specified
CNA	<a href="#">Red Hat</a>	<a href="#">Red Hat Enterprise Linux 9</a>	Not specified	Not specified
CNA	<a href="#">Red Hat</a>	<a href="#">Red Hat OpenShift Container Platform 4</a>	Not specified	Not specified

#### References

Reference	Source	Link	Tags
<a href="https://access.redhat.com/security/cve/CVE-2026-4426">access.redhat.com/security/cve/CVE-2026-4426</a>	<a href="mailto:secalert@redhat.com">secalert@redhat.com</a>	<a href="https://access.redhat.com">access.redhat.com</a>	Third Party Advisory
<a href="https://bugzilla.redhat.com/show_bug.cgi">bugzilla.redhat.com/show_bug.cgi</a>	<a href="mailto:secalert@redhat.com">secalert@redhat.com</a>	<a href="https://bugzilla.redhat.com">bugzilla.redhat.com</a>	Issue Tracking, Third Party Advisory
<a href="https://access.redhat.com/errata/RHSA-2026:8944">access.redhat.com/errata/RHSA-2026:8944</a>	<a href="mailto:secalert@redhat.com">secalert@redhat.com</a>	<a href="https://access.redhat.com">access.redhat.com</a>	
<a href="https://github.com/libarchive/libarchive/pull/2897">github.com/libarchive/libarchive/pull/2897</a>	<a href="mailto:secalert@redhat.com">secalert@redhat.com</a>	<a href="https://github.com">github.com</a>	Issue Tracking, Patch
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

#### Vendor Comments And Credit

## Discovery Credit

**CNA:** Red Hat would like to thank Elhanan Haenel for reporting this issue. (en)

### Additional Advisory Data

Source	Time	Event
CNA	2026-03-19T12:39:13.967Z	Reported to Red Hat.
CNA	2026-03-19T00:00:00.000Z	Made public.

### Workarounds

**CNA:** To mitigate this issue, avoid processing untrusted ISO9660 images with `libarchive`. Restricting the sources of ISO files and ensuring they originate from trusted entities can prevent exploitation.

There are currently no legacy QID mappings associated with this CVE.

© [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](#)