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

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-4426
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-19 15:16:28 UTC
Updated	2026-05-03 21:16:11 UTC
Description	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

ntegrity

None

vailability

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	Libarchive	Libarchive	-	All	All	All
Operating System	Redhat	Enterprise Linux	10.0	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Operating System	Redhat	Enterprise Linux	9.0	All	All	All
Application	Redhat	Hardened Images	-	All	All	All
Application	Redhat	Openshift Container Platform	4.0	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Red Hat	Red Hat Hardened Images	unaffected 3.8.7-1.hum1 * rpm	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 10	Not specified	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 6	Not specified	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 7	Not specified	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 8	Not specified	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 9	Not specified	Not specified
CNA	Red Hat	Red Hat OpenShift Container Platform 4	Not specified	Not specified

References

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