Libarchive: infinite loop denial of service in rar5 decompression via archive_read_data() in libarchive

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

Summary

CVE	CVE-2026-4111
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-13 19:55:13 UTC
Updated	2026-04-20 04:16:45 UTC
Description	A flaw was identified in the RAR5 archive decompression logic of the libarchive library, specifically within the archive_read_

Risk And Classification

Primary CVSS: v3.1 7.5 HIGH from secalert@redhat.com

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

EPSS: 0.000340000 probability, percentile 0.096550000 (date 2026-04-19)

Problem Types: CWE-835 | CWE-835 Loop with Unreachable Exit Condition ('Infinite Loop')

Version	Source	Type	Score	Severity	Vector
3.1	secalert@redhat.com	Secondary	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
3.1	CNA	CVSS	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

ntegrity

None

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Red Hat	Red Hat Enterprise Linux 10	unaffected 0:3.7.7-5.el10_1 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 10.0 Extended Update Support	unaffected 0:3.7.7-5.el10_0 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 9	unaffected 0:3.5.3-7.el9_7 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 9	unaffected 0:3.5.3-7.el9_7 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 9.0 Update Services For SAP Solutions	unaffected 0:3.5.3-2.el9_0.3 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 9.2 Update Services For SAP Solutions	unaffected 0:3.5.3-5.el9_2.1 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 9.4 Extended Update Support	unaffected 0:3.5.3-4.el9_4.2 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 9.6 Extended Update Support	unaffected 0:3.5.3-6.el9_6.1 * rpm
CNA	Red Hat	Red Hat OpenShift Container Platform 4.13	unaffected 413.92.202604080111-0 * rpm
CNA	Red Hat	Red Hat AI Inference Server 3.2	unaffected sha256:54616c9f3e4d27120504b0b2020
CNA	Red Hat	Red Hat AI Inference Server 3.3	unaffected sha256:0ec114881d9dcd28a5dbbb2ec0e
CNA	Red Hat	Red Hat AI Inference Server 3.3	unaffected sha256:813ba7ccd1696b44deb90d9e6cc
CNA	Red Hat	Red Hat AI Inference Server 3.3	unaffected sha256:be6d568f28044533e4ad80f0856
CNA	Red Hat	Red Hat Discovery 2	unaffected sha256:040dadd657afdb9f0914f896a496
CNA	Red Hat	Red Hat Discovery 2	unaffected sha256:062310de4b34e278f8c7e4634de
CNA	Red Hat	Red Hat Enterprise Linux 6	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 7	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 8	Not specified
CNA	Red Hat	Red Hat Hardened Images	Not specified

References

Reference	Source	Link	Tags
bugzilla.redhat.com/show_bug.cgi	secalert@redhat.com	bugzilla.redhat.com	
access.redhat.com/security/cve/CVE-2026-4111	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:8747	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:8865	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:6647	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:7106	secalert@redhat.com	access.redhat.com	

access.redhat.com/errata/RHSA-2026:7105	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:7329	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:8748	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:5080	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:5063	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:7335	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:7093	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:8746	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:7239	secalert@redhat.com	access.redhat.com	
github.com/libarchive/libarchive/pull/2877	secalert@redhat.com	github.com	
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	2026-03-11T11:18:51.609Z	Reported to Red Hat.
CNA	2026-03-11T00:00:00.000Z	Made public.

Workarounds

CNA: Mitigation for this issue is either not available or the currently available options don't meet the Red Hat Product Security criteria comprising ease of use and deployment, applicability to widespread installation base or stability.

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