



CVE-2026-5121

VEX [↗](#)

Public on March 30, 2026

Last modified: April 16, 2026 at 4:24:53 PM UTC



Moderate severity

What does this mean?

7.5

CVSS v3 Score Breakdown

[Jump to section](#)

Description	Statement	Mitigation	Additional information	Affected Packages	CVSS Score Details	Weakness (CWE)	Acknowledgements	FAQ
-------------	-----------	------------	------------------------	-------------------	--------------------	----------------	------------------	-----

Description

A flaw was found in `libarchive`. On 32-bit systems, an integer overflow vulnerability exists in the `zifs` block pointer allocation logic. A remote attacker can exploit this by providing a specially crafted ISO9660 image, which can lead to a heap buffer overflow. This could potentially allow for arbitrary code execution on the affected system.

Statement

Important: An integer overflow flaw in `libarchive` on 32-bit systems can lead to a heap buffer overflow. This vulnerability occurs when processing a specially crafted ISO9660 image, allowing an attacker to potentially execute arbitrary code. Red Hat Enterprise Linux 64-bit systems are not affected by this flaw.

Mitigation

To mitigate this issue, avoid processing untrusted ISO9660 images with applications that utilize `libarchive`. Users should only extract or read content from ISO images obtained from trusted sources.


Additional information

- Bugzilla 2452945: libarchive: libarchive: Arbitrary code execution via integer overflow in ISO9660 image processing
- CWE-190: Integer Overflow or Wraparound

External references

- <https://www.cve.org/CVERecord?id=CVE-2026-5121>
- <https://nvd.nist.gov/vuln/detail/CVE-2026-5121>
- <https://github.com/advisories/GHSA-2vww-vqp-v8vc>
- <https://github.com/libarchive/libarchive/pull/2934>

Affected Packages and Issued Red Hat Security Errata

 Unless explicitly stated as not affected, all previous versions of packages in any minor update stream of a product listed here should be assumed vulnerable, although may not have been subject to full analysis.

Search:

Filter by:

Products / Services ▼

Components ▼

State ▼

Errata ▼

[Clear all](#)

Products / Services	Red Hat Enterprise Linux 7 Extended Lifecycle Support
Components	libarchive
State	Fixed
Justification	None
Errata	RHSA-2026:8517
Release Date	April 16, 2026

Products / Services	Red Hat Enterprise Linux 8
Components	libarchive
State	Fixed
Justification	None
Errata	RHSA-2026:8534
Release Date	April 16, 2026

Products / Services	Red Hat Enterprise Linux 8.2 Advanced Update Support
Components	libarchive
State	Fixed
Justification	None
Errata	RHSA-2026:8521

« < 1 of 2 > »

Common Vulnerability Scoring System (CVSS) Score Details

Important note

CVSS scores for open source components depend on vendor-specific factors (e.g. version or build chain). Therefore, Red Hat's score and impact rating can be different from NVD and other vendors. Red Hat remains the authoritative CVE Naming Authority (CNA) source for its products and services (see Red Hat classifications).

CVSS v3 Score Breakdown

	Red Hat	NVD	CVE List
CVSS v3 Base Score	7.5	N/A	9.8
Attack Vector	Network	N/A	Network
Attack Complexity	Low	N/A	Low
Privileges Required	None	N/A	None
User Interaction	None	N/A	None
Scope	Unchanged	N/A	Unchanged
Confidentiality Impact	High	N/A	High
Integrity Impact	None	N/A	High
Availability Impact	None	N/A	High

CVSS v3 Vector

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

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

Acknowledgements

Red Hat would like to thank Elhanan Haenel for reporting this issue.

Frequently Asked Questions


Why is Red Hat's CVSS v3 score or Impact different from other vendors?	▼
My product is listed as "Under investigation" or "Affected", when will Red Hat release a fix for this vulnerability?	▼
What can I do if my product is listed as "Will not fix"?	▼
What can I do if my product is listed as "Fix deferred"?	▼
What is a mitigation?	▼
I have a Red Hat product but it is not in the above list, is it affected?	▼
Why is my security scanner reporting my product as vulnerable to this vulnerability even though my product version is fixed or not affected?	▼
My product is listed as "Out of Support Scope". What does this mean?	▼


Not sure what something means? Check out our [Security Glossary](#).


Want to get errata notifications? [Sign up here](#).


For clarification or corrections, please contact [Red Hat Product Security](#).


Last modified: April 16, 2026 at 4:24:53 PM UTC
CVE description copyright © 2021





Quick Links 

Help 

Site Info 

Related Sites 

 Partial system outage



- About Red Hat
- Jobs
- Events
- Locations
- Contact Red Hat
- Red Hat Blog
- Inclusion at Red Hat
- Cool Stuff Store
- Red Hat Summit

© 2026 Red Hat

[Privacy statement](#)

[Terms of use](#)

[All policies and guidelines](#)

[Digital accessibility](#)

[Cookie preferences](#)