

GitHub Advisory Database / Unreviewed / CVE-2026-5121

A flaw was found in libarchive. On 32-bit systems, an...

Critical severity Unreviewed Published 2 weeks ago to the GitHub Advisory Database • Updated 1 hour ago

Package

No package listed— Suggest a package

Affected versions

Unknown

Patched versions

Unknown

Description

A flaw was found in libarchive. On 32-bit systems, an integer overflow vulnerability exists in the zisofs 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.

References

- <https://nvd.nist.gov/vuln/detail/CVE-2026-5121>
- [libarchive/libarchive#2934](https://libarchive.org/libarchive#2934)
- <https://access.redhat.com/security/cve/CVE-2026-5121>
- https://bugzilla.redhat.com/show_bug.cgi?id=2452945
- [GHSA-2vww-vqpv-v8vc](https://ghsa.com/GHSA-2vww-vqpv-v8vc)
- <https://access.redhat.com/errata/RHSA-2026:8510>



Published by the [National Vulnerability Database](#) 2 weeks ago



Published to the GitHub Advisory Database 2 weeks ago



Last updated 1 hour ago

Severity

Critical 9.8 / 10

CVSS v3 base metrics

Attack vector	Network
Attack complexity	Low
Privileges required	None
User interaction	None
Scope	Unchanged
Confidentiality	High
Integrity	High
Availability	High

[Learn more about base metrics](#)

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

EPSS score

0.087% (25th percentile)

Weaknesses

▶ CWE-190

CVE ID

CVE-2026-5121

GHSA ID

GHSA-2vww-vqpv-v8vc

Source code

No known source code

Dependabot alerts are not supported on this advisory because it does not have a package from a supported ecosystem with an affected and fixed version.

[Learn more about GitHub language support](#)

This advisory has been edited. [See History](#).

See something to contribute? [Suggest improvements for this vulnerability](#).