



# About cookies on this site



## CVE

A cookie is a small amount of data that is sent to your browser from a web server and stored on your device. The cookie may be placed by Red Hat or by an authorized third party.

VEX [↗](#)  
Public   
Last mo

When you use this site, Red Hat uses cookies and other technologies which are necessary to enable the basic features of the site to function (Required cookies). Subject to your preferences, Red Hat and its authorized partners may also use cookies to analyze your use of the website to evaluate and improve our performance, to improve our service to you and to personalize your experience (Functional cookies) as well as advertising cookies to show you ads that are more relevant to you (Advertising cookies). We honor the preferences you select.



In addition to the services they provide to Red Hat, certain Red Hat authorized partners may also use this data for their own purposes or for

**Accept Default**

**Do Not Sell or Share My Personal Information**

[Description](#) [Mitigation](#) [Additional information](#) [CVSS Score Details](#) [Weakness \(CWE\)](#) [Acknowledgements](#) [FAQ](#)  
[Cookie Preferences](#) | [Privacy Statement](#)

## Description

A flaw was found in rsync. This vulnerability arises from a race condition during rsync's handling of symbolic links. Rsync's default behavior when encountering symbolic links is to skip them. If an attacker replaced a regular file with a symbolic link at the right time, it was possible to bypass the default behavior and traverse symbolic links. Depending on the privileges of the rsync process, an attacker could leak sensitive information, potentially leading to privilege escalation.

## Mitigation

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

## Additional information

- Bugzilla 2332968: rsync: Race Condition in rsync Handling Symbolic Links
- CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')

### External references

- <https://www.cve.org/CVERecord?id=CVE-2024-12747>
- <https://nvd.nist.gov/vuln/detail/CVE-2024-12747>
- <https://kb.cert.org/vuls/id/952657>

## 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
<b>CVSS v3 Base Score</b>	5.6	N/A	N/A

	Red Hat	NVD	CVE List
<b>Attack Vector</b>	Local	N/A	N/A
<b>Attack Complexity</b>	High	N/A	N/A
<b>Privileges Required</b>	Low	N/A	N/A
<b>User Interaction</b>	None	N/A	N/A
<b>Scope</b>	Changed	N/A	N/A
<b>Confidentiality Impact</b>	High	N/A	N/A
<b>Integrity Impact</b>	None	N/A	N/A
<b>Availability Impact</b>	None	N/A	N/A

## CVSS v3 Vector

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

## Acknowledgements

Red Hat would like to thank Aleksei Gorban "loqpa" for reporting this issue.

## Frequently Asked Questions

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

**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: January 28, 2026 at 6:57:42 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 and Do Not Sell or Share My Personal Information