




# CVE-2024-12086

VEX [↗](#)

Public on January 14, 2025

Last modified: April 14, 2026 at 9:41:26 PM UTC



**MODERATE**

**Moderate severity**

[What does this mean?](#)

**6.1**

[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 rsync. It could allow a server to enumerate the contents of an arbitrary file from the client's machine. This issue occurs when files are being copied from a client to a server. During this process, the rsync server will send checksums of local data to the client to compare with in order to determine what data needs to be sent to the server. By sending specially constructed checksum values for arbitrary files, an attacker may be able to reconstruct the data of those files byte-by-byte based on the responses from the client.

## Statement

This vulnerability marked as moderate rather than important because it requires the attacker to control the rsync server, which limits the scope of exploitation to scenarios where the client interacts with untrusted or compromised servers. Additionally, the attack is non-trivial, as it relies on

the attacker sending specially crafted checksum values and deducing file contents byte-by-byte based on the client's responses. This makes the exploit more complex and time-consuming compared to direct file access vulnerabilities. Furthermore, the impact is limited to file data enumeration, and it does not allow arbitrary code execution or privilege escalation on the client.

## 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 2330577: rsync: rsync server leaks arbitrary client files
- CWE-390: Detection of Error Condition Without Action

### External references

- <https://www.cve.org/CVERecord?id=CVE-2024-12086>
- <https://nvd.nist.gov/vuln/detail/CVE-2024-12086>
- <https://kb.cert.org/vuls/id/952657>

## 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 10
Components	rsync
State	Fixed
Justification	None
Errata	RHBA-2025:6470
Release Date	May 13, 2025

---

Products / Services	Red Hat Enterprise Linux 6
Components	rsync
State	Out of support scope
Justification	None
Errata	
Release Date	

---

Products / Services	Red Hat Enterprise Linux 7
Components	rsync
State	Out of support scope
Justification	None
Errata	

« < 1 of 1 > »

## 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>	6.1	6.8	N/A
<b>Attack Vector</b>	Network	Network	N/A
<b>Attack Complexity</b>	High	High	N/A
<b>Privileges Required</b>	None	None	N/A
<b>User Interaction</b>	Required	None	N/A
<b>Scope</b>	Changed	Changed	N/A
<b>Confidentiality Impact</b>	High	High	N/A
<b>Integrity Impact</b>	None	None	N/A
<b>Availability Impact</b>	None	None	N/A

## CVSS v3 Vector

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

**NVD:** CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:N/A:N

## Understanding the Weakness (CWE)

## CWE-390

### Integrity,Other


**Technical Impact:**Varies by Context; Unexpected State; Alter Execution Logic


An attacker could utilize an ignored error condition to place the system in an unexpected state that could lead to the execution of unintended logic and could cause other unintended behavior.

## Acknowledgements

Red Hat would like to thank Jasiel Spelman (Google), Pedro Gallegos (Google), and Simon Scannell (Google) 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 14, 2026 at 9:41:26 PM UTC  
CVE description copyright © 2021



The image shows a dark-themed navigation bar for the Red Hat website. On the left is the Red Hat logo, consisting of a red fedora hat icon and the text "Red Hat". On the right are social media icons for LinkedIn, YouTube, Facebook, and X. Below the logo and icons is a vertical list of four menu items: "Quick Links", "Help", "Site Info", and "Related Sites". Each menu item has a small white downward-pointing chevron icon to its right.

 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](#)