CVE

VEX
Public or
Last moc

Insigh

View

Description ments FAQ

Cookie Preferences and Opt-Out Rights
Your Choices About Cookies on this Site

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.

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 targeted advertising. This activity may qualify as a "sale" or “targeted advertising” under certain data protection laws. You can make choices using the buttons below to allow or prevent such uses.

Accept default will keep your preferences set to accept all cookies (Required, Functional and Advertising), which enables us to provide you a personalized web experience and more relevant ads on third party websites. This means that you allow our partners to collect and use this data.

Required Cookies only will set your cookie preferences to "Required Cookies" only. This will prevent our partners from collecting and using this data but may also prevent us from providing you a personalized web experience and more relevant ads on third party websites. Cookie preferences will provide further information and allow you to customize your cookie settings. Setting your cookie preferences to "Required Cookies only" will opt you out of "sales" and "targeted advertising".

Clearing your browser cookies may delete your cookie preferences. If you re-visit this site after clearing browser cookies, you will need to reset your preferences at that time. If you have set your browser’s global privacy settings, then we recognize the global privacy settings from your browser.

Descr

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
CVSS v3 Base Score	6.1	6.8	N/A
Attack Vector	Network	Network	N/A
Attack Complexity	High	High	N/A
Privileges Required	None	None	N/A
User Interaction	Required	None	N/A
Scope	Changed	Changed	N/A
Confidentiality Impact	High	High	N/A
Integrity Impact	None	None	N/A
Availability Impact	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

⚠ Partial system outage