CVE-2024-12088

VEX

Public on January 14, 2025

Last modified: January 28, 2026 at 6:57:42 PM UTC

MODERATE

Moderate severity

What does this mean?

6.5

CVSS v3 Score Breakdown

Insights vulnerability analysis

View exposed systems →

Jump to section

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

Description

A flaw was found in rsync. When using the `--safe-links` option, the rsync client fails to properly verify if a symbolic link destination sent from the server contains another symbolic link within it. This results in a path traversal vulnerability, which may lead to arbitrary file write outside the desired directory.

Statement

The vulnerability requires user interaction to be triggered, as the rsync client must first establish a connection/have access to the malicious rsync server (at least anonymous read-access).

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 2330676: rsync: --safe-links option bypass leads to path traversal
- CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

External references

- https://www.cve.org/CVERecord?id=CVE-2024-12088
- https://nvd.nist.gov/vuln/detail/CVE-2024-12088
- 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 8
Components	rsync
State	Fixed
Justification	None
Errata	RHSA-2025:2600
Release Date	March 11, 2025

Products / Services	Red Hat Enterprise Linux 9
Components	rsync
State	Fixed
Justification	None
Errata	RHSA-2025:7050

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	6.5	7.5	N/A
Attack Vector	Network	Network	N/A
Attack Complexity	Low	Low	N/A
Privileges Required	None	None	N/A
User Interaction	Required	None	N/A
Scope	Unchanged	Unchanged	N/A
Confidentiality Impact	None	None	N/A
Integrity Impact	High	High	N/A
Availability Impact	None	None	N/A

CVSS v3 Vector

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

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

Understanding the Weakness (CWE)

CWE-22

Integrity,Confidentiality,Availability

Technical Impact: Execute Unauthorized Code or Commands

The attacker may be able to create or overwrite critical files that are used to execute code, such as programs or libraries.

Integrity

Technical Impact: Modify Files or Directories

The attacker may be able to overwrite or create critical files, such as programs, libraries, or important data. If the targeted file is used for a security mechanism, then the attacker may be able to bypass that mechanism. For example, appending a new account at the end of a password file may allow an attacker to bypass authentication.

Confidentiality

Technical Impact: Read Files or Directories

The attacker may be able read the contents of unexpected files and expose sensitive data. If the targeted file is used for a security mechanism, then the attacker may be able to bypass that mechanism. For example, by reading a password file, the attacker could conduct brute force password guessing attacks in order to break into an account on the system.

Availability

Technical Impact: DoS: Crash, Exit, or Restart

The attacker may be able to overwrite, delete, or corrupt unexpected critical files such as programs, libraries, or important data. This may prevent the product from working at all and in the case of protection mechanisms such as authentication, it has the potential to lock out product users.

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: January 28, 2026 at 6:57:42 PM UTC