CVE

VEX

Public o

Last mo

Insigh

View

Descript ts 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,

Descr

A flaw was found in rsync which could be triggered when rsync compares file checksums. This flaw allows an attacker to manipulate the checksum length (s2length) to cause a comparison between a checksum and uninitialized memory and leak one byte of uninitialized stack data at a time.

Statement

This vulnerability is rated as having Important impact as it helps bypass Address Space Lay out Randomization (ASLR). ASLR is a memory protection system which makes the exploit ation of memory corruption vulnerabilities more difficult.

Mitigation

Seeing as this vulnerability relies on information leakage coming from the presence of data in the uninitialized memory of the `sum2` buffer, a potential mitigation involves compiling rsync with the `-ftrivial-auto-var-init=zero` option set. This mitigates the issue because it initializes the `sum2` variable's memory with zeroes to prevent uninitialized memory disclosure.

Additional information

- Bugzilla 2330539: rsync: Info Leak via Uninitialized Stack Contents
- CWE-908: Use of Uninitialized Resource

External references

- https://www.cve.org/CVERecord?id=CVE-2024-12085
- https://nvd.nist.gov/vuln/detail/CVE-2024-12085
- 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
CVSS v3 Base Score	7.5	N/A	N/A
Attack Vector	Network	N/A	N/A
Attack Complexity	Low	N/A	N/A
Privileges Required	None	N/A	N/A
User Interaction	None	N/A	N/A
Scope	Unchanged	N/A	N/A
Confidentiality Impact	High	N/A	N/A
Integrity Impact	None	N/A	N/A
Availability Impact	None	N/A	N/A

CVSS v3 Vector

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

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?

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: September 25, 2025 at 4:28:24 PM UTC