Rsync contains six vulnerabilities

Vulnerability Note VU#952657

Original Release Date: 2025-01-14 | Last Revised: 2025-08-25

Overview

Rsync, a versatile file-synchronizing tool, contains six vulnerabilities present within versions 3.3.0 and below. Rsync can be used to sync files between remote and local computers, as well as storage devices. The discovered vulnerabilities include heap-buffer overflow, information leak, file leak, external directory file-write,–safe-links bypass, and symbolic-link race condition.

Description

Many backup programs, such as Rclone, DeltaCopy, and ChronoSync use Rsync as backend software for file synchronization. Rsync can also be used in Daemon mode and is widely used in in public mirrors to synchronize and distribute files efficiently across multiple servers. Following are the discovered vulnerabilities:

CVE-2024-12084 A heap-buffer-overflow vulnerability in the Rsync daemon results in improper handling of attacker-controlled checksum lengths (s2length). When the MAX_DIGEST_LEN exceeds the fixed

ABOUT VULNERABILITY NOTES

CONTACT US ABOUT THIS VULNERABILITY

PROVIDE A VENDOR STATEMENT

SUM_LENGTH (16 bytes), an attacker can write out-of-bounds in the sum2 buffer.

CVE-2024-12085 When Rsync compares file checksums, a vulnerability in the Rsync daemon can be triggered. An attacker could manipulate the checksum length (s2length) to force a comparison between the checksum and uninitialized memory and leak one byte of uninitialized stack data at a time.

CVE-2024-12086 A vulnerability in the Rsync daemon could cause a server to leak the contents of arbitrary files from clients' machines. This happens when files are copied from client to server. During the process, a malicious Rsync server can generate invalid communication tokens and checksums from data the attacker compares. The comparison will trigger the client to ask the server to resend data, which the server can use to guess a checksum. The server could then reprocess data, byte to byte, to determine the contents of the target file.

CVE-2024-12087 A path traversal vulnerability in the Rsync daemon affects the --inc-recursive option, a default-enabled option for many flags that can be enabled by the server even if not explicitly enabled by the client. When using this option, a lack of proper symlink verification coupled with de-duplication checks occurring on a per-file-list basis could allow a server to write files outside of the client's intended destination directory. A malicious server could remotely trigger this activity by exploiting symbolic links named after valid client directories/paths.

CVE-2024-12088 A --safe-links option vulnerability results in Rsync failing to properly verify whether the symbolic link destination contains another symbolic link within it. This results in a path traversal vulnerability, which may lead to arbitrary files being written outside of the desired directory.

CVE-2024-12747 Rsync is vulnerable to a symbolic-link race condition, which may lead to privilege escalation. A user could gain access to privileged files on affected servers.

Impact

When combined, the first two vulnerabilities (heap buffer overflow and information leak) allow a client to execute arbitrary code on a device that has an Rsync server running. The client requires only anonymous read-access to the server, such as public mirrors. Additionally, attackers can take control of a malicious server and read/write arbitrary files of any connected client. Sensitive data, such as SSH keys, can be extracted, and malicious code can be executed by overwriting files such as ~/.bashrc or ~/.popt.

Solution

Apply the latest patches available at https://github.com/RsyncProject/rsync and https://download.samba.org/pub/rsync/src/. Users should run updates on their software as soon as possible. As Rsync can be distributed bundled, ensure any software that provides such updates is also kept current to address these vulnerabilities.

Acknowledgements

Thanks to Simon Scannell, Pedro Gallegos, and Jasiel Spelman at Google Cloud Vulnerability Research for discovering the first five vulnerabilities; thanks to Aleksei Gorban for discovering the symbolic-link race condition. Finally, thanks to Andrew Tridgell for reporting all of them. This document was written by Dr. Elke Drennan, CISSP.

Vendor Information

AlmaLinux OS Foundation	Affected
Arch Linux	Affected
Gentoo Linux	Affected
NixOS	Affected
Red Hat	Affected
SUSE Linux	Affected
Triton Data Center	Affected
Afero	Not Affected
AMD	Not Affected
Arista Networks	Not Affected

View all 79 vendors

Other Information

CVE IDs:	CVE-2024-12084 CVE-2024-12085 CVE-2024-12086 CVE-2024-12087 CVE-2024-12088 CVE-2024-12747
API URL:	VINCE JSON | CSAF
Date Public:	2025-01-14
Date First Published:	2025-01-14
Date Last Updated:	2025-08-25 17:26 UTC

Document Revision: 11

Sponsored by CISA.

Download PGP Key

Read CERT/CC Blog

Learn about Vulnerability Analysis

Carnegie Mellon University
Software Engineering
Institute
4500 Fifth Avenue
Pittsburgh, PA 15213-2612
412-268-5800

Contact SEI

Contact CERT/CC

412-268-5800
cert@cert.org