

HiveForce Labs

THREAT ADVISORY

 **VULNERABILITY REPORT**

Rsync Vulnerabilities Could Spell Disaster for Over 660,000 Servers

Date of Publication

January 20, 2025

Admiralty Code

A1

TA Number

TA2025013

Summary

First Seen: January 14, 2025

Affected Product: Rsync

Impact: Rsync, a widely used utility for file synchronization in Unix-like systems, has become the focus of serious security concerns, with over 660,000 servers potentially exposed to critical vulnerabilities. These flaws, including the severe CVE-2024-12084, could allow attackers to execute arbitrary code, leak sensitive data, and manipulate files without authentication. As the risk landscape intensifies, organizations must reassess their security measures to protect against these escalating threats.

CVEs

CVE	NAME	AFFECTED PRODUCTS	ZERO-DAY	CISA	MICRO PATCH
CVE-2024-12084	Rsync Heap Buffer Overflow Vulnerability	Rsync			
CVE-2024-12085	Rsync Information Disclosure Vulnerability	Rsync			
CVE-2024-12086	Rsync Information Disclosure Vulnerability	Rsync			
CVE-2024-12087	Rsync Path Traversal Vulnerability	Rsync			
CVE-2024-12088	Rsync Path Traversal Vulnerability	Rsync			
CVE-2024-12747	Rsync Information Disclosure Vulnerability	Rsync			

Vulnerability Details

#1

Rsync short for Remote Sync is a robust utility extensively employed for transferring and synchronizing files between local and remote systems. Predominantly used in Unix-like operating environments, rsync is lauded for its efficiency and flexibility, particularly in incremental data transfers. Despite its widespread adoption, over 660,000 rsync servers are potentially vulnerable to critical security flaws, significantly elevating the threat landscape.

#2

The most severe of these, CVE-2024-12084, enables remote code execution (RCE) via a heap buffer overflow triggered by improper checksum length handling. An attacker can exploit this vulnerability by dispatching maliciously crafted requests to a rsync server, thereby executing arbitrary code on the host system without authentication. This presents an acute risk, particularly for organizations permitting anonymous read access, which could inadvertently facilitate full system compromise.

#3

CVE-2024-12085 further exacerbates the risk by allowing information disclosure from the server's memory, potentially leaking sensitive data such as API keys or user credentials. Exploiting this flaw, an adversary might harvest critical information to escalate their privileges or gain deeper access.

#4

In environments where users might connect to malicious rsync servers either by deception or oversight vulnerabilities like CVE-2024-12086 could lead to the inadvertent exposure of sensitive files, such as SSH keys or configuration files, compounding the security implications.

#5

Moreover, CVE-2024-12087 and CVE-2024-12088 introduce path traversal vulnerabilities that allow unauthorized file manipulations. An attacker could craft exploits to inject malicious scripts into critical directories or create unsafe symbolic links, redirecting file operations to sensitive filesystem areas. This could result in unauthorized access, file tampering, or further exploitation of critical system resources.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-12084	Rsync 3.2.7 or higher, and lower than 3.4.0.	cpe:2.3:a:rsync:rsync:*:*:*:*:*:*:*:*	CWE-122
CVE-2024-12085	Rsync versions earlier than 3.4.0.		CWE-119
CVE-2024-12086	Rsync versions earlier than 3.4.0.		CWE-390
CVE-2024-12087	Rsync versions earlier than 3.4.0.		CWE-35
CVE-2024-12088	Rsync versions earlier than 3.4.0.		CWE-35
CVE-2024-12747	Rsync versions earlier than 3.4.0.		CWE-362

Recommendations



Immediate Upgrade to rsync 3.4.0: All organizations should upgrade their rsync installations to version 3.4.0 as soon as it becomes available, as this version contains patches for all the identified vulnerabilities (CVE-2024-12084 to CVE-2024-12747). Use the command `dpkg -l rsync` to verify the installed version and ensure it has been updated.



Temporary Mitigations for CVE-2024-12084: Disable SHA Support, recompile rsync with the flags `CFLAGS=-DDISABLE_SHA512_DIGEST` and `CFLAGS=-DDISABLE_SHA256_DIGEST` to mitigate the risk of the heap buffer overflow. Restrict Network Access by ensuring that rsync servers are not exposed to the internet by blocking or restricting TCP port 873 at the firewall or security group level, reducing the attack surface.



Mitigations for CVE-2024-12085: Recompile rsync using `-ftrivial-auto-var-init=zero` to prevent information leakage by zeroing the stack contents.



Vulnerability Management: This involves regularly assessing and updating software to address known vulnerabilities. Maintain an inventory of software versions and security patches, and evaluate the security practices of third-party vendors, especially for critical applications and services.

Potential **MITRE ATT&CK** TTPs

<u>TA0002</u> Execution	<u>TA0003</u> Persistence	<u>TA0004</u> Privilege Escalation	<u>TA0007</u> Discovery
<u>T1059</u> Command and Scripting Interpreter	<u>T1190</u> Exploit Public-Facing Application	<u>T1203</u> Exploitation for Client Execution	<u>T1036</u> Masquerading
<u>T1005</u> Data from Local System	<u>T1068</u> Exploitation for Privilege Escalation	<u>T1040</u> Network Sniffing	<u>T1213</u> Data from Information Repositories
<u>T1078</u> Valid Accounts	<u>T1210</u> Exploitation of Remote Services		

Patch Details

Upgrade to rsync 3.4.0 to patch all identified vulnerabilities, including CVE-2024-12084 through CVE-2024-12747.

Link:

<https://download.samba.org/pub/rsync/src/>

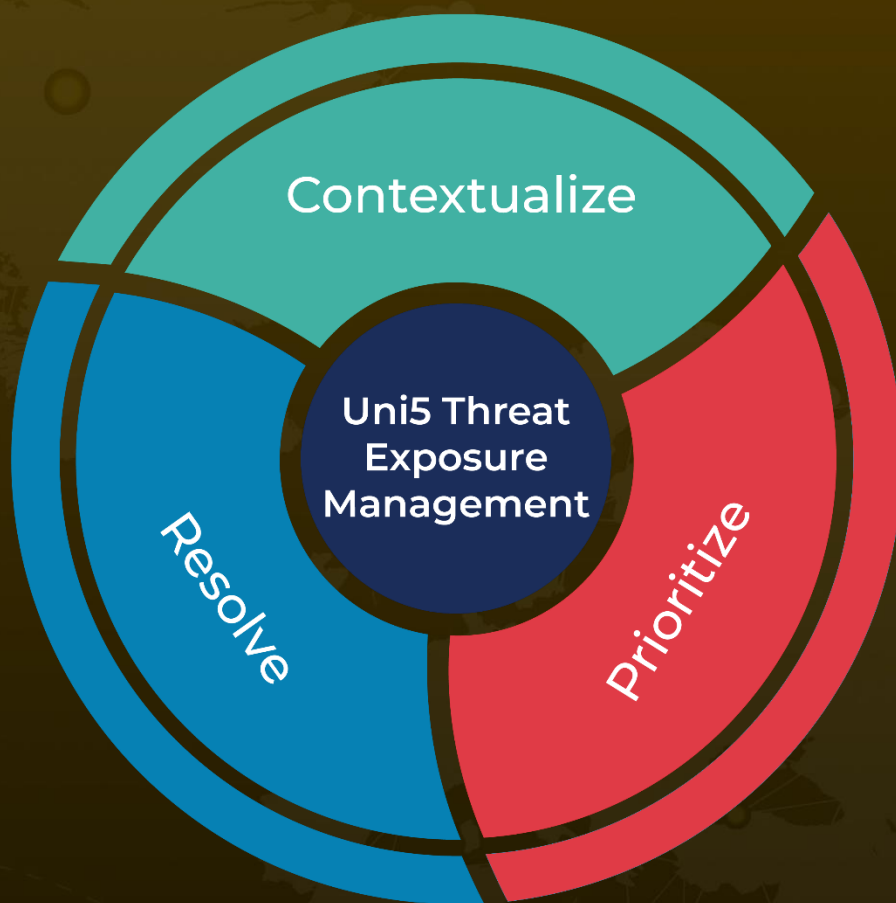
References

<https://www.openwall.com/lists/oss-security/2025/01/14/3>

What Next?

At Hive Pro, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with HivePro Uni5: Threat Exposure Management Platform.



REPORT GENERATED ON

January 20, 2025 • 9:30 PM

© 2025 All Rights are Reserved by HivePro



More at www.hivepro.com