مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Multiple Vulnerabilities in Rsync Servers

Tracking #:432316756

Date:17-01-2025

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed multiple vulnerabilities have been discovered in Rsync, an open-source file synchronization tool, affecting over 660,000 servers.

TECHNICAL DETAILS:

Multiple vulnerabilities have been discovered in Rsync, an open-source file synchronization tool, affecting over 660,000 servers. These flaws, including a critical heap-buffer overflow (CVE-2024-12084), allow remote attackers to execute arbitrary code, access sensitive files, and potentially compromise systems.

Vulnerability Details:

- CVE-2024-12084-Critical (CVSS: 9.8)-Heap Buffer Overflow vulnerability arising from improper handling of checksum lengths in the Rsync daemon, leading to out-of-bounds writes in the buffer.
- CVE-2024-12085- Severity: High (CVSS: 7.5)-Information Leak via Uninitialized Stack
- CVE-2024-12086)-Severity: Moderate (CVSS: 6.1)-Server Leaks Arbitrary Client Files
- CVE-2024-12087- Severity: Moderate (CVSS: 6.5)-Path Traversal via --inc-recursive Option
- CVE-2024-12088- Severity: Moderate (CVSS: 6.5)-Bypass of --safe-links Option
- CVE-2024-12747- Severity: Medium (CVSS: 5.6)-Symbolic Link Race Condition

- **Fixed Version:** Upgrade to Rsync 3.4.0 or higher

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to Update Rsync Server to the fixed version or latest.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://access.redhat.com/security/cve/cve-2024-12084#cve-cvss-v3