CVE-2025-23120: REMOTE CODE EXECUTION FOR DOMAIN USERS IN VEEAM

Vairav CVE Report

Date: March 21st, 2025

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Phone: +977 4541540

Thirbam Sadak 148
Baluwatar, Kathmandu

Mobile: +977-9820105900

Email: sales@vairavtech.com

EXECUTIVE SUMMARY

A critical vulnerability, **CVE-2025-23120**, has been identified in Veeam Backup & Replication software. This flaw allows authenticated domain users to execute arbitrary code remotely, posing a significant risk of system compromise. The vulnerability has been assigned a **CVSS v3.1 score of 9.9**, indicating its critical severity.

VULNERABILITY DETAILS

CVE-2025-23120

- **Description:** The vulnerability arises from improper deserialization handling within Veeam Backup & Replication. Authenticated domain users can exploit this flaw to execute arbitrary code on the affected system. Notably, this issue is prevalent in environments where the backup server is joined to an Active Directory domain, a configuration against Veeam's security best practices.
- **Impact:** Successful exploitation allows attackers to perform remote code execution, potentially leading to full system compromise, data loss, or service disruption.
- **CVSS Score:** 9.9 (Critical)

AFFECTED VERSIONS

- **Veeam Backup & Replication** version 12.3.0.310 and all earlier version 12 builds

Unsupported product versions were not tested but are likely affected and should be considered vulnerable.

EXPLOIT DETAILS

In domain-joined environments, any authenticated domain user can exploit this vulnerability to execute arbitrary code on the backup server. This scenario is particularly concerning in large organizations where numerous users have domain credentials, increasing the attack surface. Exploitation could lead to full system compromise, data loss, or service disruption.

RECOMMENDED ACTIONS

Patch & Upgrade:

Upgrade to the latest Veeam Backup & Replication version:

- 12.3.1 (build 12.3.1.1139)

For deployments currently running Veeam Backup & Replication 12.3 (build 12.3.0.310), a hotfix is available for customers who cannot immediately update to version 12.3.1.

ADDITIONAL SECURITY MEASURES

- **Configuration Review**: Ensure that backup servers are not joined to Active Directory domains, aligning with Veeam's security best practices.
- **Access Controls**: Restrict access to backup servers to essential personnel only, minimizing potential attack vectors.
- **Network Segmentation**: Isolate backup servers from general network traffic to limit exposure.

REFERENCES

- https://www.bleepingcomputer.com/news/security/veeam-rce-bug-lets-domain-users-hack-backup-servers-patch-now/
- https://labs.watchtowr.com/by-executive-order-we-are-banning-blacklists-domain-level-rce-in-veeam-backup-replication-cve-2025-23120/
- https://www.veeam.com/kb4724

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

Website: https://vairavtech.com