مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

Critical Remote Code Execution Vulnerabilities in Veeam Backup & Replication

Tracking #:432317814

Date:15-10-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Veeam Software has released a critical security update addressing multiple vulnerabilities affecting Veeam Backup & Replication and Veeam Agent for Microsoft Windows.

TECHNICAL DETAILS:

Veeam Software has released a critical security update addressing multiple vulnerabilities affecting Veeam Backup & Replication and Veeam Agent for Microsoft Windows. Two of these vulnerabilities—CVE-2025-48983 and CVE-2025-48984—can be exploited to achieve Remote Code Execution (RCE) on domain-joined backup servers by an authenticated domain user, posing a severe risk to enterprise backup infrastructures.
A third vulnerability, CVE-2025-48982, allows Local Privilege Escalation (LPE) through the restoration of malicious files on systems using Veeam Agent for Microsoft Windows.

Vulnerabilities Overview

1. CVE-2025-48983 — Remote Code Execution in Mount Service

- **Severity:** Critical (CVSS 9.9)
- **Impact:** Remote Code Execution on backup infrastructure hosts.
- **Attack Vector:** Authenticated domain user can exploit the Mount service in Veeam Backup & Replication.
- **Affected Versions:**
  - Veeam Backup & Replication 12.3.2.3617 and earlier 12.x builds.
- **Notes:**
  - Impacts only **domain-joined** backup infrastructure servers.
  - The upcoming **Veeam v13** and **Veeam Software Appliance** are **not affected**.
- **Fixed in:** 12.3.2.4165.

2. CVE-2025-48984 — Remote Code Execution on Backup Server

- **Severity:** Critical (CVSS 9.9)
- **Impact:** Remote Code Execution on the Backup Server by an authenticated domain user.
- **Attack Vector:** Abuse of authenticated network access to compromise domain-joined Veeam servers.
- **Affected Versions:**
  - Veeam Backup & Replication 12.3.2.3617 and earlier 12.x builds.
- **Notes:**
  - Impacts **domain-joined** backup servers only.
  - Not applicable to the Veeam Software Appliance or upcoming v13 builds.
- **Fixed in:** 12.3.2.4165.

3. CVE-2025-48982 — Local Privilege Escalation in Veeam Agent

- **Severity:** High (CVSS 7.3)
- **Impact:** Privilege escalation via malicious file restoration.
- **Attack Vector:** Exploitation requires social engineering or administrative action restoring an attacker-crafted file.
- **Affected Versions:**
  - Veeam Agent for Microsoft Windows 6.3.2.1205 and earlier 6.x builds.
- **Fixed in:** Veeam Agent for Microsoft Windows 6.3.2.1302.

RECOMMENDATIONS:

Apply Security Updates Immediately:

- Upgrade Veeam Backup & Replication and Veeam Agent for Microsoft Windows to fixed version or later.

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://www.veeam.com/kb4771