Security Advisory 2025-038

Critical Vulnerabilities in Veeam Backup

2025-10-15 — v1.0

TLP:CLEAR

History:

- *15/10/2025 — v1.0 – Initial publication*

Summary

On October 14, 2025, Veeam released a security advisory addressing multiple vulnerabilities including 2 critical in its Veeam Backup product [1].

CERT-EU recommends updating affected software as soon as possible and following Veeam implementation best practices [2].

Technical Details

The vulnerability **CVE-2025-48983**, with a CVSS score of 9.9, resides in the Mount service of Veeam Backup & Replication and allows an authenticated domain user to execute arbitrary code on backup infrastructure hosts.

The vulnerability **CVE-2025-48984**, with a CVSS score of 9.9, allows an authenticated domain user to execute arbitrary code remote code execution (RCE) on the Backup Server.

The vulnerability **CVE-2025-48982**, with a CVSS score of 7.3, resides in Veeam Agent for Microsoft Windows and allows for Local Privilege Escalation if a system administrator is tricked into restoring a malicious file.

Affected Products

The vulnerabilities **CVE-2025-48983** and **CVE-2025-48984** impact Veeam Backup & Replication 12.3.2.3617 and all earlier version 12 builds. They only impact domain-joined backup servers.

The vulnerability **CVE-2025-48982** impacts Veeam Agent for Microsoft Windows 6.3.2.1205 and all earlier version 6 builds.

The vendor mentions that unsupported product versions are not tested, but are likely affected and should be considered vulnerable.

Recommendations

It is recommended updating affected products as soon as possible and following Veeam implementation best practices [2].

References

[1] https://www.veeam.com/kb4771

[2] https://bp.veeam.com/security/Design-and-implementation/Hardening/Workgroup_or_Domain.html#best-practice