CERT-EU 10 years

Security Advisory 2025-021

Critical Vulnerability in Veeam Backup & Replication

2025-06-18 — v1.0

TLP:CLEAR

History:

- *18/06/2025 — v1.0 – Initial publication*

Summary

On 17 June 2025, Veeam released an advisory addressing several vulnerabilities in Veeam Backup & Replication, one of which is rated as critical [1].

It is recommended updating as soon as possible.

Technical Details

The vulnerability **CVE-2025-23121**, with a CVSS score of 9.9, is a flaw allowing remote code execution (RCE) on the Backup Server by an authenticated domain user. This vulnerability only impacts domain-joined backup servers.

It is said that this vulnerability is likely a bypass of the fix, released in March 2025, addressing the vulnerability **CVE-2025-23120** [2,3].

Affected Products

This vulnerability impacts Veeam Backup & Replication version 12 builds, including 12.3.1.1139 (addressed in 12.3.2 (build 12.3.2.3617)).

The vendor notes that unsupported product versions are not tested, but are likely affected and should be considered vulnerable [1].

Recommendations

It is recommended updating as soon as possible, and implementing best practices provided by the vendor [4].

References

[1] https://www.veeam.com/kb4743

[2] https://thehackernews.com/2025/06/veeam-patches-cve-2025-23121-critical.html

[3] https://thehackernews.com/2025/03/veeam-and-ibm-release-patches-for-high.html

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