Security Advisory 2024-092

Critical Vulnerability in Veeam

September 6, 2024 — v1.0

TLP:CLEAR

History:

- *06/09/2024 — v1.0 – Initial publication*

Summary

On September 5, 2024, Veeam disclosed a critical remote code execution (RCE) vulnerability tracked as **CVE-2024-40711**, affecting Veeam Backup & Replication (VBR) [1]. This flaw allows unauthenticated attackers to execute arbitrary code on vulnerable systems (CVSS score: 9.8). VBR is a target for ransomware attacks, as it plays a key role in enterprise data protection.

Users are advised to update to version 12.2.0.334 as soon as possible.

Technical Details

The vulnerability tracked as **CVE-2024-40711** enables remote, unauthenticated code execution on vulnerable VBR systems, potentially leading to lateral movement and full infrastructure compromise.

Affected Products

- Veeam Backup & Replication versions 12.1.2.172 and earlier.

Recommendations

CERT-EU recommends updating to VBR version 12.2.0.334 as soon as possible.

References

[1] https://www.bleepingcomputer.com/news/security/veeam-warns-of-critical-rce-flaw-in-backup-and-replication-software/