

Alert Bulletin

Bulletin N.:

Publication Date: 10/06/2026

Subject: Alert 2026-62 Critical Vulnerability in Veeam Backup & Replication

Traffic Light Protocol (TLP): Amber

Affected Product(s):

- Veeam Backup & Replication 12.x

Description

Veeam released security updates to fix the critical vulnerability **CVE-2026-44963** with a **CVSS v4 9.4**, which allows an authenticated user within the Windows domain to execute remote code (Remote Code Execution – RCE) on the backup server.

An attacker who compromises a domain account with limited privileges could exploit this flaw to gain control over the Veeam server, manipulate backup tasks, access sensitive information, alter backups, or use the compromised platform as a foothold to perform lateral movements within the corporate network. Because backup servers often store critical information for operational recovery, this type of vulnerability represents a priority target for ransomware groups and advanced malicious actors.

Solution:

- Update Veeam Backup & Replication to version 12.3.2.4854 or higher.

Additional Information:

- <https://www.bleepingcomputer.com/news/security/new-veeam-vulnerability-exposes-backup-servers-to-rce-attacks/>