Critical Vulnerability in Veeam Backup & Replication Could Allow Remote Code Execution

***Author**: Portia S. Cole – CTI Researcher*

TL;DR

Veeam has released security updates for a critical vulnerability (CVE-2026-44963) affecting Veeam Backup & Replication 12.x.

The flaw could allow an authenticated domain user with low privileges to execute code remotely on a backup server, potentially leading to full system compromise.

Overview

There is a critical remote code execution vulnerability (CVE-2026-44963, CVSS 9.4) affecting Veeam Backup & Replication that could allow an authenticated domain user to execute code on a backup server.

Affected Products

- Veeam Backup & Replication 12.3.2.4465 and earlier Version 12 builds

Not Affected:

- Veeam Backup & Replication 13.x

Veeam Backup & Replication is a backup and disaster recovery platform used to protect, recover, and manage data across physical, virtual, and cloud environments. The platform is commonly used by organizations to support business continuity, ransomware recovery, and long-term data protection.

CVE-2026-44963 affects domain-joined backup servers and could allow a low-privileged domain user to execute code on the affected system. Successful exploitation could provide an attacker with control of backup infrastructure, potentially allowing them to disable or delete backups, access sensitive data, harvest credentials, and disrupt recovery operations.

Backup servers are frequently targeted by ransomware and extortion groups because they often have elevated privileges and broad access to critical systems and stored data. Compromising backup infrastructure can significantly increase recovery times and reduce an organization's ability to restore operations following a cyberattack.

Veeam has stated that it is not aware of active exploitation at this time. However, the company warns that threat actors may attempt to reverse engineer the patch and target unpatched systems following public disclosure.

Organizations operating backup and disaster recovery infrastructure that relies on Veeam Backup & Replication may be affected.

Aspire Protects

- **Patch** – Upgrade to Veeam Backup & Replication version 12.3.2.4854 or later. See Veeam's security advisory for more information.
- Prioritize patching domain-joined Veeam backup servers.
- Review access controls for backup administrators and service accounts.
- Monitor for unusual authentication activity involving backup infrastructure.
- Verify backup integrity and recovery procedures.
- Maintain immutable or offline backups where possible.

TTPs

Execution

- Command and Scripting Interpreter [T1059] – A threat actor could execute arbitrary code on the vulnerable Veeam Backup Server.

Impact

- Inhibit System Recovery [T1490] – A threat actor could delete, modify, or disable backups to hinder recovery efforts.

IoCs

There are no known IoCs at this time. Aspire is actively monitoring and will notify customers if any are found. For more details on how we can help protect your organization, contact Aspire's Customer Success Management team.

Targeted Industries

Organizations operating backup and disaster recovery infrastructure that relies on Veeam Backup & Replication may be affected.

- Education
- Energy
- Finance
- Healthcare
- Legal
- Manufacturing
- Public Sector
- Retail

Aspire Service Offerings

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors.
  - Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyber attacks.
- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.
  - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

Supporting Documentation

KB4869: Vulnerability Resolved in Veeam Backup & Replication 12.3.2.4854