An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

NCSC #2603130218

NCSC Advisory

Multiple Vulnerabilities in Veeam Products

16th, March 2026

STATUS: TLP:CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.

Description

CVE ID: CVE-2026-21666, CVE-2026-21667, CVE-2026-21668, CVE-2026-21672, CVE-2026-21708, CVE-2026-21669, CVE-2026-21671

Published: 2026-03-12

Vendor: Veeam

CVE-2026-21666

Products Affected

Product	Version
Backup and Replication	< 12.3.2.4465

Impact

A vulnerability allowing an authenticated domain user to perform remote code execution (RCE) on the Backup Server.

- **CVSS Score[1]:** 9.9
- **Common Weakness Enumeration (CWE)[2]:** CWE-284 Improper Access Control
- **Known Exploited Vulnerability (KEV) catalog:** No
- **Used by Ransomware Operators:** N/A

CVE-2026-21667

Products Affected

Product	Version
Backup and Replication	< 12.3.2.4465

[1] https://www.first.org/cvss/

[2] https://cwe.mitre.org

Impact

A vulnerability allowing an authenticated domain user to perform remote code execution (RCE) on the Backup Server.

- **CVSS Score:** 9.9
- **Common Weakness Enumeration (CWE):** CWE-284 Improper Access Control
- **Known Exploited Vulnerability (KEV) catalog**: No
- **Used by Ransomware Operators**: N/A

CVE-2026-21668

Products Affected

Product	Version
Backup and Replication	< 12.3.2.4465

Impact

A vulnerability allowing an authenticated domain user to bypass restrictions and manipulate arbitrary files on a Backup Repository.

- **CVSS Score:** 8.8
- **Known Exploited Vulnerability (KEV) catalog**: No
- **Used by Ransomware Operators**: N/A

CVE-2026-21672

Products Affected

Product	Version
Backup and Replication	< 12.3.2.4465
Backup and Replication	< 13.0.1.2067

Impact

A vulnerability allowing local privilege escalation on Windows-based Veeam Backup & Replication servers.

- **CVSS Score:** 8.8
- **Known Exploited Vulnerability (KEV) catalog**: No
- **Used by Ransomware Operators**: N/A

CVE-2026-21708

Products Affected

Product	Version
Backup and Replication	< 12.3.2.4465
Backup and Replication	< 13.0.1.2067

Impact

A vulnerability allowing a Backup Viewer to perform remote code execution (RCE) as the postgres user.

- **CVSS Score:** 9.9
- **Known Exploited Vulnerability (KEV) catalog**: No
- **Used by Ransomware Operators**: N/A

CVE-2026-21669

Products Affected

Product	Version
Backup and Replication	< 13.0.1.2067

Impact

A vulnerability allowing an authenticated domain user to perform remote code execution (RCE) on the Backup Server.

- **CVSS Score:** 9.9
- **Known Exploited Vulnerability (KEV) catalog**: No
- **Used by Ransomware Operators**: N/A

CVE-2026-21671

Products Affected

Product	Version
Backup and Replication	< 13.0.1.2067

Impact

A vulnerability allowing an authenticated user with the Backup Administrator role to perform remote code execution (RCE) in high availability (HA) deployments of Veeam Backup & Replication.

- **CVSS Score:** 9.1
- **Known Exploited Vulnerability (KEV) catalog**: No
- **Used by Ransomware Operators**: N/A

Recommendations

The NCSC strongly recommends installing updates for vulnerable systems with the highest priority, after thorough testing. Affected organisations should review the latest release notes and install the relevant updates from Veeam.

- https://www.veeam.com/kb4830
- https://www.veeam.com/kb4831
- https://nvd.nist.gov/vuln/detail/CVE-2026-21666
- https://nvd.nist.gov/vuln/detail/CVE-2026-21667
- https://nvd.nist.gov/vuln/detail/CVE-2026-21668
- https://nvd.nist.gov/vuln/detail/CVE-2026-21672
- https://nvd.nist.gov/vuln/detail/CVE-2026-21708
- https://nvd.nist.gov/vuln/detail/CVE-2026-21669
- https://nvd.nist.gov/vuln/detail/CVE-2026-21671