An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

NCSC #2606160520

NCSC Advisory

Veeam: Backup and Replication

CVE-2026-44963

17th, June 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-2026-44963

Published: 2026-06-09

Vendor: Veeam

Product: Backup and Replication

CVSS Score[1]: 9.4

Products Affected

Product	Version
Backup and Replication	0 < 12.3.2

Impact

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

Common Weakness Enumeration (CWE)[2]: CWE-502: Deserialization of Untrusted Data

Known Exploited Vulnerability (KEV) catalog[3]: No

Used by Ransomware Operators: N/A

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

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

[3] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

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://nvd.nist.gov/vuln/detail/CVE-2026-44963
- https://www.cve.org/CVERecord?id=CVE-2026-44963
- https://www.veeam.com/kb4869