An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

NCSC #2506190094

NCSC Advisory

Critical Vulnerability in Veeam Backup and Recovery

CVE-2025-23121

19th, June 2025

STATUS: TLP:CLEAR

Description

CVE ID: CVE-2025-23121

Published: 2025-06-18

Vendor: Veeam

Product: Backup and Recovery

CVSS Score[1]: 9.9

Products Affected

Product	Version
Backup and Recovery	12.3.1 <= 12.3.1

Impact

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

Common Weakness Enumeration (CWE)[2]: N/A

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-2025-23121
- https://www.cve.org/CVERecord?id=CVE-2025-23121
- https://www.veeam.com/kb4743