



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

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.

TLP: CLEAR

An Roinn Comhshaoil,
Aeráide agus Cumarsáide
Department of the Environment,
Climate and Communications



Description

CVE ID: CVE-2025-23121

Published: 2025-06-18

Vendor: Veeam

Product: Backup and Recovery

CVSS Score¹: 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) catalog³: 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>



TLP: CLEAR

An Roinn Comhshaoil,
Aeráide agus Cumarsáide
Department of the Environment,
Climate and Communications



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>

