VULNERABILITY BULLETINS

Multiple Vulnerabilities Addressed in Veeam Backup & Replication Solution

TLP:WHITE

Jan 07, 2026

On January 6, 2026, Veeam released security updates to address four vulnerabilities affecting its Backup & Replication solution, the most severe of which could allow unauthenticated privilege escalation, enabling the launch of remote code execution (RCE) attacks.

Tracked as CVE-2025-59470, CVE-2025-55125, CVE-2025-59469, and CVE-2025-59468, these flaws impact all version 13 builds prior to the latest release. Organizations are strongly urged to apply the available patches as soon as possible to prevent potential system compromise and data loss.

Health-ISAC provides this information to increase situational awareness and encourage organizations to assess their level of risk to these vulnerabilities.

Analysis

The most critical vulnerability in this set is CVE-2025-59470, which carries a CVSS score of 9.0. This flaw resides in the way the application processes specific parameters; specifically, a threat actor

can achieve remote code execution (RCE) as the postgres user by sending a malicious interval or order parameter. While technically a critical-range CVSS score, Veeam has adjusted the severity to High for practical purposes because exploitation requires the attacker to already possess the privileges of a Backup Operator or Tape Operator.

Similarly, CVE-2025-55125 and CVE-2025-59469 (both CVSS 7.2) present high-severity risks to the backup infrastructure. Exploitation of CVE-2025-55125 allows a Backup or Tape Operator to perform RCE as the root user by creating a malicious backup configuration file. Meanwhile, CVE-2025-59469 enables users with those same operator roles to perform unauthorized file writes as the root user. Both vulnerabilities effectively bridge the gap between a restricted operator role and full administrative control over the underlying operating system.

The fourth vulnerability, CVE-2025-59468 (CVSS 6.7), is classified as medium severity and impacts Backup Administrators. An attacker with this role can perform RCE as the postgres user by sending a malicious password parameter. Due to the flaws being triggered via internal parameters and configuration files, the primary condition for exploitation is an authenticated session with one of these highly privileged, yet theoretically restricted, service roles.

These vulnerabilities specifically affect Veeam Backup & Replication 13.0.1.180 and all earlier version 13 builds. Notably, Veeam has confirmed that previous major versions, such as the 12.x branch, are not impacted by this specific group of flaws. At this time, there are no reports of these vulnerabilities being exploited in the wild; however, the security flaws are of concern given that Veeam infrastructure is a frequent target for ransomware groups seeking to disable recovery options.

Recommendations and Mitigations

Health-ISAC recommends organizations review and assess their level of risk to these vulnerabilities and implement the following:

- Apply updates to affected solutions to Veeam Backup version 13.0.1.1071 or later.
- Review and audit accounts assigned the Backup Operator, Tape Operator, and Backup Administrator roles.
  - Ensure they are restricted to only necessary personnel and service accounts.
- Follow Veeam's recommended Security Best Practices, including:
  - Isolating backup infrastructure from the production domain
  - Restricting network access to the Backup Server to trusted IP addresses only.
- Monitor Infrastructure
  - Implement logging and alerting for unusual activities on the backup server.
- Reviewing the Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients Resources.

Reference(s)	securityweek, veeam, hhs, bleepingcomputer

Alert ID 65df8295

View Alert

Share Feedback

was this helpful? |

Tags CVE-2025-59468, CVE-2025-59469, CVE-2025-55125, CVE-2025-59470, Veeam Backup & Replication Software, Veeam

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Access the Health-ISAC Threat Intelligence Portal

Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Health-ISAC Threat Intelligence Portal (HTIP).

For Questions or Comments

Please email us at toc@h-isac.org

Download Health-ISAC's Information Sharing App.  

For more updates and alerts, visit: **https://health-isac.cyware.com/webapp/**