**Date Posted: 2026/03/19**

# [Vulnerability Alert] Multiple Critical Security Vulnerabilities Found in Veeam Backup Software

- Subject Explanation: [Vulnerability Alert] Multiple Critical Security Vulnerabilities Found in Veeam Backup Software

- Content Description:
  - Forwarding Taiwan Computer Emergency Response Team / Coordination Center (TWCERT/CC) Security Alert TWCERTCC-200-202603-00000015
  - Veeam Backup and Replication is Veeam's core backup software. Recently, Veeam released a critical security vulnerability advisory.
  - [CVE-2026-21666, CVSS: 9.9] Allows authenticated domain users to remotely execute code on the backup server.
  - [CVE-2026-21667, CVSS: 9.9] Allows authenticated domain users to remotely execute code on the backup server.
  - [CVE-2026-21668, CVSS: 8.8] Allows authenticated domain users to bypass restrictions and manipulate arbitrary files in the backup repository.
  - [CVE-2026-21672, CVSS: 8.8] A local privilege escalation vulnerability exists in Windows-based Veeam Backup and Replication servers.
  - [CVE-2026-21708, CVSS: 9.9] Allows backup viewers to remotely execute code as users.
  - [CVE-2026-21669, CVSS: 9.9] Allows authenticated domain users to remotely execute code on the backup server.
  - [CVE-2026-21671, CVSS: 9.1] Allows authenticated users with the backup administrator role to remotely execute code in High Availability (HA) deployments of Veeam Backup and Replication.
- Impacted Platforms:
  - Veeam Backup and Replication versions 12.3.2.4165 and earlier
  - Veeam Backup and Replication versions 13.0.1.1071 and earlier
- Suggested Measures:
  - Please update to the following versions: Veeam Backup and Replication version 12.3.2.4465, Veeam Backup and Replication version 13.0.1.2067
- References:
  1. https://www.twcert.org.tw/tw/cp-169-10783-d40f5-1.html

---

Computer and Communication Center
Network Systems Division

From:
https://net.nthu.edu.tw/netsys/ - **網路系統組**

Permanent link:
**https://net.nthu.edu.tw/netsys/en:mailing:announcement:20260319_28**

Last update: **2026/03/19 16:26**