مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Remote Code Execution Vulnerability in Veeam Backup & Replication

Tracking #:432319107

Date:10-06-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability in Veeam Backup & Replication that could allow remote code execution (RCE) on affected backup servers.

TECHNICAL DETAILS:

Vulnerability Details

- **CVE-2026-44963**
- **Severity:** Critical | **CVSS:** 9.4 (CVSS v4)
- A remote code execution vulnerability exists in Veeam Backup & Replication that allows an authenticated domain user to execute arbitrary code on the backup server. The vulnerability only affects domain-joined backup servers and may enable attackers to gain control of the backup environment, disrupt operations, or access sensitive data.
- Successful exploitation could allow arbitrary code execution on affected backup servers, potentially resulting in unauthorized access, data compromise, and disruption of backup and recovery operations.

Affected Products and Versions

- Veeam Backup & Replication 12.3.2.4465 and all earlier version 12 builds
- All earlier Version 12 builds (12, 12.1, 12.2, 12.3, 12.3.1, and 12.3.2)

Fixed Versions

- Veeam Backup & Replication 12.3.2.4854 and later

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released by Veeam.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://www.veeam.com/kb4869