مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

Critical Vulnerability in Veeam Backup & Replication

Tracking #:432316827

Date:05-02-2025

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cybersecurity Council has observed critical vulnerability has been discovered within the Veeam Updater component used in several Veeam Backup & Replication appliances.

TECHNICAL DETAILS:

A critical vulnerability (CVE-2025-23114) has been identified in the Veeam Updater component used by several Veeam backup products. This vulnerability allows attackers to execute arbitrary code with root-level permissions through a Man-in-the-Middle attack. The issue affects multiple Veeam products, including Veeam Backup for Salesforce, Nutanix AHV, AWS, Microsoft Azure, Google Cloud, and Oracle Linux Virtualization Manager/Red Hat Virtualization.

Vulnerability Details:

- CVE ID: CVE-2025-23114
- Severity: Critical
- CVSS v3.1 Score: 9.0
- Attack Vector: Man-in-the-Middle
- Impact: Arbitrary code execution with root-level permissions

Patched Veeam Updater Component Versions:

- Veeam Backup for Salesforce: 7.9.0.1124
- Veeam Backup for Nutanix AHV: 9.0.0.1125
- Veeam Backup for AWS: 9.0.0.1126
- Veeam Backup for Microsoft Azure: 9.0.0.1128
- Veeam Backup for Google Cloud: 9.0.0.1128
- Veeam Backup for Oracle Linux Virtualization Manager and Red Hat Virtualization: 9.0.0.1127

RECOMMENDATIONS:

- Immediate Patching: All affected customers should prioritize upgrading to the latest versions of the Veeam Updater component.
- Verify Current Versions: Organizations should confirm the current version of the Veeam Updater component on their systems. This can be done through the built-in Veeam Updater or by checking the version within the appliance's update history.
- Network Segmentation: To reduce the risk of Man-in-the-Middle attacks, ensure that all Veeam appliances are placed within properly secured and segmented networks, using secure communication protocols.
- Enable Automatic Updates: Enable and configure automatic updates for all Veeam appliances to ensure that future vulnerabilities are quickly addressed.

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/kb4712