مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerability in Veeam Backup Enterprise Manager

Tracking #:432315883

Date:23-05-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Veeam has released a security advisory to address a critical vulnerability in Veeam Backup Enterprise Manager (VBEM).

TECHNICAL DETAILS:

Veeam has released a security advisory to address a critical vulnerability and other three vulnerabilities in Veeam Backup Enterprise Manager (VBEM).

Vulnerabilities addressed:

- **CVE-2024-29849 – 9.8 Critical-** This vulnerability in Veeam Backup Enterprise Manager allows an unauthenticated attacker to log in to the Veeam Backup Enterprise Manager web interface as any user.
- **CVE-2024-29850 (CVSS score: 8.8),**which allows account takeover via NTLM relay
- **CVE-2024-29851 (CVSS score: 7.2),** which allows a privileged user to steal NTLM hashes of a Veeam Backup Enterprise Manager service account if it's not configured to run as the default Local System account.
- **CVE-2024-29852 (CVSS score: 2.7),** which allows a privileged user to read backup session logs.

Fixed Version:

- Veeam Backup Enterprise Manager 12.1.2.172

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to apply the security patch as soon as possible.

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/kb4581