مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

High-Severity Vulnerability in Veeam Backup Enterprise Manager

Tracking #:432316484

Date:07-11-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a high-severity vulnerability in Veeam Backup Enterprise Manager (VBEM) that could be exploited to gain unauthorized access, potentially compromising the integrity and confidentiality of backup data and configurations.

TECHNICAL DETAILS:

Vulnerabilities Details:

- **CVE-2024-40715**
- Severity: High
- CVSS v3.1 Score: 7.7
- The vulnerability allows attackers to bypass authentication in Veeam Backup Enterprise Manager while performing a Man-in-the-Middle (MITM) attack. This could potentially lead to unauthorized access to sensitive backup data and configurations.
- Successful exploitation of this vulnerability could allow attackers to gain unauthorized access to backup data, modify backup configurations, and compromise the integrity of backup systems.

Affected Products:

- Veeam Backup Enterprise Manager (VBEM) version 12.2.0.334 and earlier

Mitigation:

- For Veeam Backup Enterprise Manager 12.2.0.334:
  - Apply the hotfix provided in Veeam KB4682
- For Veeam Backup Enterprise Manager 12.1.2.172 or older:
  - Upgrade to version 12.2.0.334 using the latest Veeam Backup & Replication ISO

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the mitigation or workaround provided 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/kb4682