مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

Security Updates - Veeam Products

Tracking #:432316585

Date:04-12-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Veeam has released security updates to patch multiple high-severity vulnerabilities in Veeam Backup & Replication and Veeam Agent for Microsoft Windows.

TECHNICAL DETAILS:

Multiple high-severity vulnerabilities have been discovered in Veeam Backup & Replication and Veeam Agent for Microsoft Windows. These vulnerabilities (CVE-2024-40717, CVE-2024-42451, CVE-2024-42452, CVE-2024-42453, CVE-2024-42455, CVE-2024-42456, CVE-2024-42457, CVE-2024-45204, CVE-2024-45207) allow authenticated users with assigned roles to perform various malicious actions, including executing scripts with elevated privileges, accessing saved credentials, uploading files to connected hosts, modifying configurations, and exploiting insecure deserialization. The vulnerabilities have CVSS v3.1 scores ranging from 7.0 to 8.8, indicating high severity.

Vulnerabilities Details:

1. CVE-2024-40717
   - Severity: High (CVSS v3.1: 8.8)
   - Description: Allows execution of scripts with elevated privileges via pre-job or post-job tasks.
   - Impact: Potential system compromise through unauthorized privilege escalation.
2. CVE-2024-42451
   - Severity: High (CVSS v3.1: 7.7)
   - Description: Enables access to all saved credentials in human-readable format.
   - Impact: Potential exposure of sensitive authentication information.
3. CVE-2024-42452
   - Severity: High (CVSS v3.1: 8.8)
   - Description: Permits remote file upload to connected ESXi hosts with elevated privileges.
   - Impact: Possible compromise of connected virtual infrastructure.
4. CVE-2024-42453
   - Severity: High (CVSS v3.1: 8.8)
   - Description: Allows modification of connected virtual infrastructure host configurations.
   - Impact: Potential disruption or compromise of virtual environments.
5. CVE-2024-42455
   - Severity: High (CVSS v3.1: 7.1)
   - Description: Enables exploitation of insecure deserialization, leading to file deletion with service account privileges.
   - Impact: Possible data loss or system instability.
6. CVE-2024-42456
   - Severity: High (CVSS v3.1: 8.8)
   - Description: Grants access to privileged methods and control of critical services.
   - Impact: Potential for significant system compromise and service disruption.
7. CVE-2024-42457
   - Severity: High (CVSS v3.1: 7.7)
   - Description: Allows exposure of saved credentials through remote management interface methods.

- Impact: Risk of credential theft and unauthorized access.

8. CVE-2024-45204
   - Severity: High (CVSS v3.1: 7.7)
   - Description: Exploits insufficient permissions in credential handling, potentially leaking NTLM hashes.
   - Impact: Increased risk of credential compromise and lateral movement.
9. CVE-2024-45207
   - Severity: High (CVSS v3.1: 7.0)
   - A vulnerability could lead to a DLL injection attack when the PATH environment variable is altered to include directories where an attacker can write files.

Affected versions:

- Veeam Backup & Replication 12.2.0.334 and all earlier version 12 builds.
- Veeam Agent for Microsoft Windows 6.2 and all earlier version 6 builds.(CVE-2024-45207)

Fixed Versions:

- Veeam Backup & Replication 12.3 (build 12.3.0.310)
- Veeam Agent for Microsoft Windows 6.3 (build 6.3.0.177) — Included with Veeam Backup & Replication 12.3

RECOMMENDATIONS:

Upgrade Veeam Backup & Replication to the latest fixed version to patch the identified vulnerabilities.

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/kb4693