



مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



Critical Vulnerability in Veeam Service Provider Console

Tracking #:432316591

Date:05-12-2024

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 INTELLIGENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Veeam has disclosed two significant vulnerabilities affecting its Service Provider Console (VSPC), including a critical remote code execution (RCE) flaw.

TECHNICAL DETAILS:

Veeam has disclosed two significant vulnerabilities affecting its Service Provider Console (VSPC), including a critical remote code execution (RCE) flaw. These vulnerabilities, CVE-2024-42448 and CVE-2024-42449, impact VSPC versions 8.1.0.21377 and earlier, including versions 8 and 7. The critical vulnerability (CVE-2024-42448) has a CVSS v3.1 score of 9.9, allowing potential RCE on the VSPC server machine. The high-severity vulnerability (CVE-2024-42449) enables attackers to leak NTLM hashes and delete files on the VSPC server.

1. CVE-2024-42448

- Severity: **Critical**
- CVSS v3.1 Score: 9.9
- Impact: Allows remote code execution on the VSPC server machine from an authorized VSPC management agent.
- Affected Versions: VSPC 8.1.0.21377 and all earlier versions of 8 and 7 builds.

2. CVE-2024-42449

- Severity: High
- CVSS v3.1 Score: 7.1
- Impact: Enables leaking of NTLM hash of the VSPC server service account and file deletion on the VSPC server machine
- Affected Versions: Same as CVE-2024-42448

Fixed Versions:

- Veeam Service Provider Console 8.1.0.21999

RECOMMENDATIONS:

- Immediately upgrade Veeam Service Provider Console to fixed version or later to mitigate both vulnerabilities.
- Ensure that only authorized personnel and systems have access to the VSPC management agent. Review and minimize the access privileges to limit the potential impact of any exploit.

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/kb4679>