



مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



Remote Code Execution Vulnerability in Veeam Service Provider Console
Tracking #:432315833
Date:08-05-2024

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 a High Severity vulnerability in Veeam Service Provider Console (VSPC) allows attackers to remotely execute code on vulnerable systems.

TECHNICAL DETAILS:

Vulnerability Details:

- **Vulnerability: CVE-2024-29212** (CVSS v3.1 Score: 8.8)
- Due to an unsafe deserialization method used by the Veeam Service Provider Console (VSPC) server in communication between the management agent and its components, under certain conditions, it is possible to perform Remote Code Execution (RCE) on the VSPC server machine.

Fixed Versions:

- Veeam Service Provider Console 7.0.0.18899
- Veeam Service Provider Console 8.0.0.19236

RECOMMENDATIONS:

Organizations using Veeam Service Provider Console should prioritize patching the vulnerability and implement stricter access controls to mitigate the risk.

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/kb4575>