



مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



Critical Vulnerability in ConnectWise ScreenConnect
Tracking #:432318629
Date:19-03-2026

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 critical vulnerability in ScreenConnect that could be exploited to gain unauthorized access to affected systems.

TECHNICAL DETAILS:

ConnectWise ScreenConnect addresses a vulnerability in the handling of server-level cryptographic material.

In affected versions, machine keys were stored in server configuration files, which under certain conditions could allow unauthorized access and misuse for session authentication. Version 26.1 introduces improved protections, including encrypted storage and enhanced key management, reducing the risk of exploitation.

Vulnerability Details

- **CVE ID:** CVE-2026-3564
- **Severity:** Critical **CVSS Score:** 9.0
- This vulnerability is caused by improper protection and verification of cryptographic signatures. An attacker may exploit this flaw to extract machine keys from configuration files and use them to forge or hijack authenticated sessions. While exploitation requires specific conditions, a successful attack could result in unauthorized access, data compromise, and potential full system impact.

Affected Versions

- ScreenConnect versions prior to 26.1

Fixed Versions

On-Premise Deployments

- ScreenConnect 26.1 and later

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released by ConnectWise.

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.connectwise.com/company/trust/security-bulletins/2026-03-17-screenconnect-bulletin>