



مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



High-Severity Vulnerability in ConnectWise ScreenConnect
Tracking #:432317139
Date:28-04-2025

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 ConnectWise ScreenConnect that could potentially be exploited to execute malicious code on affected systems.

TECHNICAL DETAILS:

ConnectWise has identified and addressed a critical security vulnerability in ScreenConnect versions 25.2.3 and earlier. This vulnerability, tracked as CVE-2025-3935, could potentially allow for remote code execution (RCE) on affected servers.

Vulnerability Details

- **CVE-2025-3935**
- CVSS Score: 8.1 High
- The vulnerability exists due to the way ScreenConnect utilizes ASP.NET's ViewState mechanism. ASP.NET Web Forms use ViewState to maintain control and page states across web requests. This data is Base64-encoded and protected using machine keys.
- A successful exploit requires an attacker to first obtain the server's machine keys. If these keys are compromised, an attacker could then craft a malicious ViewState payload and send it to the ScreenConnect server. This could lead to the execution of arbitrary code on the server.

Affected Systems:

- **On-Premises ScreenConnect:** All versions up to and including 25.2.3.

Fixed Versions:

- ScreenConnect version 25.2.4 or 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://nvd.nist.gov/vuln/detail/CVE-2025-3935>