مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerabilities in ConnectWise Automate
Tracking #:432317829
Date:17-10-2025

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed ConnectWise has released a critical security update for its Automate remote monitoring and management (RMM) platform, addressing a critical and high severity vulnerabilities that could allow attackers to intercept agent communications or inject malicious updates into managed environments.

TECHNICAL DETAILS:

ConnectWise has released a critical security update for its Automate remote monitoring and management (RMM) platform, addressing a critical and high severity vulnerabilities that could allow attackers to intercept agent communications or inject malicious updates into managed environments.

The vulnerabilities, tracked as CVE-2025-11492 and CVE-2025-11493, affect all ConnectWise Automate versions prior to 2025.9. Exploitation could lead to unauthorized code execution, data interception, or remote compromise of managed systems — posing significant risk to MSPs and enterprise IT operations.

Vulnerability Overview

1. **CVE-2025-11492 CVSS:3.1 9.6** Cleartext Transmission of Sensitive Information
2. **CVE-2025-11493 CVSS:3.1 8.8** Download of Code Without Integrity Check

Affected Versions
- ConnectWise Automate versions prior to 2025.9

Remediation
- **Cloud:** Cloud instances have already been updated to the latest Automate release.
- **On-prem:** Apply the 2025.9 release.

RECOMMENDATIONS:

- Immediate Patch Deployment- Upgrade all on-premises ConnectWise Automate installations to fixed version or later.

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/connectwise-automate-2025.9-security-fix