VULNERABILITY BULLETINS

Security Update Released for ConnectWise Automate Vulnerabilities

TLP:WHITE

Oct 17, 2025

On October 16, 2025, ConnectWise released a security update to address two high-severity vulnerabilities, CVE-2025-11492 and CVE-2025-11493, that could enable adversary-in-the-middle (AiTM) attacks.

These flaws allow threat actors to intercept sensitive agent communications and inject malicious code or updates, primarily affecting on-premise deployments. While cloud instances have already been updated, all users running affected on-premise versions of ConnectWise Automate are strongly advised to apply the 2025.9 patch as soon as possible to enforce secure communication protocols.

Health-ISAC is sharing this update to increase situational awareness and encourage organizations to assess their level of risk to these vulnerabilities.

Analysis

ConnectWise Automate is a remote monitoring and management (RMM) platform widely utilized by managed service providers

(MSPs), third-party IT service companies, and internal IT departments within large enterprises. As a central management hub, Automate agents operate with high privileges across several client machines, giving it deep control over patching, configuration, and endpoint management. Due to its pervasive access and high privileges, the security of Automate is paramount, as a compromise can lead to widespread organizational breaches for both the provider and their end users.

The vulnerabilities addressed include CVE-2025-11492, which carries a critical CVSS score of 9.6 and allows cleartext transmission of sensitive Information. This flaw permits Automate agents, particularly in on-prem environments, to communicate over insecure HTTP channels rather than encrypted HTTPS. The second vulnerability, CVE-2025-11493, has a CVSS score of 8.8 and lacks proper integrity verification of checksums or digital signatures on update packages, their dependencies, or integrations.

Exploiting these two flaws in combination allows a network-based adversary to execute a adversary-in-the-middle (AiTM) attacks. By intercepting unencrypted traffic, the threat actor can impersonate a legitimate ConnectWise server and exploit the lack of integrity checks to substitute malicious updates or code. This can lead to the remote deployment of malware, exfiltration of credentials and sensitive data, or complete system compromise across all managed endpoints, posing a severe risk to service continuity and client security.

The affected versions are ConnectWise Automate versions prior to 2025.9. ConnectWise has released the Automate 2025.9 version to fully address both vulnerabilities by enforcing HTTPS for all agent communications, thus mitigating the risk of cleartext interception and improving the security surrounding updates. Cloud-hosted instances of ConnectWise Automate have already been updated and require no user action. However, users running on-premise servers should apply the 2025.9 release to obtain the patch.

Recommendations and Mitigations

Health-ISAC recommends organizations review and assess their level of risk to this vulnerability and implement the following:

- Applying the security update to affected on-premise instances.
- Verifying and enforcing the use of TLS 1.2 or higher for all agent communications to ensure secure data transmission across the network.
- Reviewing the Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients Resources.

Reference(s)	nist, hhs, bleepingcomputer, connectwise, nist 1

Alert ID 64450926

View Alert

Share Feedback

was this helpful? |

Tags Remote Monitoring and Management, CVE-2025-11493, CVE-2025-11492, RMM, ConnectWise Automate, ConnectWise

Access the Health-ISAC Threat Intelligence Portal

Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps.

Contact membership@h-isac.org for access to Health-ISAC Threat Intelligence Portal (HTIP).

For Questions or Comments

Please email us at toc@h-isac.org

Download Health-ISAC's Information Sharing App.  

For more updates and alerts, visit: **https://health-isac.cyware.com/webapp/**