Unencrypted Client-Server Communication in ConnectWise Automate™ Solution Center

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-6066
State	PUBLISHED
Assigner	ConnectWise
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-20 16:16:50 UTC
Updated	2026-04-20 19:05:30 UTC
Description	ConnectWise has released a security update for ConnectWise Automate™ that addresses a behavior in the ConnectWise A

Risk And Classification

Primary CVSS: v3.1 7.1 HIGH from 7d616e1a-3288-43b1-a0dd-0a65d3e70a49

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:N

EPSS: 0.000130000 probability, percentile 0.019760000 (date 2026-04-22)

Problem Types: CWE-319 | CWE-319 CWE-319 Cleartext transmission of sensitive information

Version	Source	Type	Score	Severity	Vector
3.1	7d616e1a-3288-43b1-a0dd-0a65d3e70a49	Secondary	7.1	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:N
3.1	CNA	CVSS	7.1	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

ntegrity

Low

Availability

None

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:N

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	ConnectWise	Automate	affected All versions prior to 2026.4	Not specified

References

Reference	Source	Lin
www.connectwise.com/company/trust/security-bulletins/2026-04-20-connectwise-autom...	7d616e1a-3288-43b1-a0dd-0a65d3e70a49	ww
CVE Program record	CVE.ORG	ww
NVD vulnerability detail	NVD	nvd

No vendor comments have been submitted for this CVE.

Additional Advisory Data

Solutions

CNA: Remediation Cloud: No action is required. On-Premise: Apply the 2026.4 release. For instruction on updating to the newest release, please reference this doc: Automate Release Notes Version 2026 - ConnectWise https://docs.connectwise.com/ConnectWise_Automate_Documentation/100/Automate_Release After applying the update, on-premises customers must ensure the following configurations are in place: * An SSL certificate is bound to the Solution Center on port 8484 to establish secure communication. Refer to the ConnectWise documentation for configuration steps: Solution Center Client and Service HTTPS Update - ConnectWise * In some environments, antivirus or endpoint protection products may interfere with the Automate patch installer or service behavior during upgrades. If issues are encountered during installation or startup, refer to the ConnectWise documentation for recommended antivirus exclusions: Automate Antivirus Exclusions for Windows https://docs.connectwise.com/ConnectWise_Automate_Documentation/060/040/010 * Ensure that the LTShare has a minimum of 1 GB of free disk space prior to installation. If you experience issues completing the update or required configuration steps, please contact ConnectWise Support for assistance.

There are currently no legacy QID mappings associated with this CVE.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**