



CVE-2023-25719

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2023-25719
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-02-13 20:15:00 UTC
Updated	2023-03-05 20:15:00 UTC
Description	ConnectWise Control before 22.9.10032 (formerly known as ScreenConnect) fails to validate user-supplied parameters suc

Risk And Classification

Problem Types: CWE-74

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Connectwise	Control	All	All	All	All

References

Reference

- Clearing the Air: Overblown Claims of Vulnerabilities, Exploits & Severity
- Hijacking Connectwise Control & Screen Connect (v.22.9.10032, MULTIPLE) for Fun and Profit - From DDoS to Multi-OS RCE! - CYBIR - Cyt
- The Importance of Responsible Security Disclosures
- MSP Technology | IT Management Software | ConnectWise
- CVE Program record
- NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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

this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)