



# CVE-2023-20178

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2023-20178
<b>State</b>	PUBLIC
<b>Assigner</b>	psirt@cisco.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-06-28 15:15:00 UTC
<b>Updated</b>	2024-01-25 17:15:00 UTC
<b>Description</b>	A vulnerability in the client update process of Cisco AnyConnect Secure Mobility Client Software for Windows and Cisco Se

## Risk And Classification

**Problem Types:** CWE-276

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Anyconnect Secure Mobility Client	All	All	All	All
Application	Cisco	Secure Client	All	All	All	All

## References

### Reference

- Cisco AnyConnect Secure Mobility Client Software for Windows and Cisco Secure Client Software for Windows Privilege Escalation Vulnerability
- CVE Program record
- NVD vulnerability detail

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[378559](#) Cisco AnyConnect Secure Mobility Client Software and Cisco Secure Client Software for Windows Privilege Escalation Vulnerability (cisco-sa-ac-csc-privesc-wx4U4Kw)

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](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)