



# CVE-2023-20241

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2023-20241
<b>State</b>	RESERVED
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-11-22 17:15:00 UTC
<b>Updated</b>	2024-01-25 17:15:00 UTC
<b>Description</b>	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new

## Risk And Classification

**Problem Types: CWE-125**

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Anyconnect Secure Mobility Client	4.9.00086	All	All	All
Application	Cisco	Anyconnect Secure Mobility Client	4.9.01095	All	All	All
Application	Cisco	Anyconnect Secure Mobility Client	4.9.02028	All	All	All
Application	Cisco	Anyconnect Secure Mobility Client	4.9.03047	All	All	All
Application	Cisco	Anyconnect Secure Mobility Client	4.9.03049	All	All	All
Application	Cisco	Anyconnect Secure Mobility Client	4.9.04043	All	All	All
Application	Cisco	Anyconnect Secure Mobility Client	4.9.04053	All	All	All
Application	Cisco	Anyconnect Secure Mobility Client	4.9.05042	All	All	All
Application	Cisco	Anyconnect Secure Mobility Client	4.9.06037	All	All	All
Application	Cisco	Secure Client	4.10.00093	All	All	All
Application	Cisco	Secure Client	4.10.01075	All	All	All
Application	Cisco	Secure Client	4.10.02086	All	All	All
Application	Cisco	Secure Client	4.10.03104	All	All	All
Application	Cisco	Secure Client	4.10.04065	All	All	All
Application	Cisco	Secure Client	4.10.04071	All	All	All
Application	Cisco	Secure Client	4.10.05085	All	All	All
Application	Cisco	Secure Client	4.10.05095	All	All	All

Application	Cisco	Secure Client	4.10.05111	All	All	All
Application	Cisco	Secure Client	4.10.06079	All	All	All
Application	Cisco	Secure Client	4.10.06090	All	All	All
Application	Cisco	Secure Client	4.10.07061	All	All	All
Application	Cisco	Secure Client	4.10.07062	All	All	All
Application	Cisco	Secure Client	4.10.07073	All	All	All
Application	Cisco	Secure Client	5.0.00238	All	All	All
Application	Cisco	Secure Client	5.0.00529	All	All	All
Application	Cisco	Secure Client	5.0.00556	All	All	All
Application	Cisco	Secure Client	5.0.01242	All	All	All
Application	Cisco	Secure Client	5.0.02075	All	All	All
Application	Cisco	Secure Client	5.0.03072	All	All	All
Application	Cisco	Secure Client	5.0.03076	All	All	All

## References

Reference	Source	Link	Tags
sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-accsc-...		<a href="https://sec.cloudapps.cisco.com">sec.cloudapps.cisco.com</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[379030](#) Cisco Secure Client Software Denial of Service (DoS) Vulnerabilities (cisco-sa-accsc-dos-9SLzkZ8)

[379484](#) Cisco Secure Client (formerly AnyConnect) Software Denial of Service (DoS) Vulnerabilities (cisco-sa-accsc-dos-9SLzkZ8) (CVE-2023-20241)

© CVE.report 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to 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](https://cve.report/api)

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