



CVE-2023-27395

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

Summary

CVE	CVE-2023-27395
State	PUBLIC
Assigner	talos-cna@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-10-12 16:15:00 UTC
Updated	2023-10-18 17:58:00 UTC
Description	A heap-based buffer overflow vulnerability exists in the vpnserver WpcParsePacket() functionality of SoftEther VPN 4.41-97

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Softether	Vpn	4.41-9782	beta	All	All
Application	Softether	Vpn	5.01.9674	All	All	All
Application	Softether	Vpn	5.02	All	All	All

References

Reference

- 2023/06/30: SE202301: Security Advisory: CVE-2023-27395 etc: Fixed 6 vulnerabilities of SoftEther VPN in cooperation with Cisco Systems, I
- TALOS-2023-1735 || Cisco Talos Intelligence Group - Comprehensive Threat Intelligence
- TALOS-2023-1735 || Cisco Talos Intelligence Group - Comprehensive Threat Intelligence
- CVE Program record
- NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[691200](#) Free Berkeley Software Distribution (FreeBSD) Security Update for softethervpn (d821956f-1753-11ee-ad66-1c61b4739ac9)

© [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](#)

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