



# CVE-2023-23581

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

## Summary

|                        |  |
|------------------------|--|
| <b>CVE</b>             | CVE-2023-23581   |
| <b>State</b>           | PUBLIC   |
| <b>Assigner</b>        | talos-cna@cisco.com  |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback   |
| <b>Published</b>       | 2023-10-12 16:15:00 UTC  |
| <b>Updated</b>         | 2023-10-18 02:46:00 UTC  |
| <b>Description</b>     | A denial-of-service vulnerability exists in the vpnserver EnSafeHTTPHeaderValueStr functionality of SoftEther VPN 5.01.9674. |

## Risk And Classification

**Problem Types:** CWE-125

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor                    | Product             | Version   | Update | Edition | Language |
|-------------|---------------------------|---------------------|-----------|--------|---------|----------|
| Application | <a href="#">Softether</a> | <a href="#">Vpn</a> | 5.01.9674 | All    | All     | All      |
| Application | <a href="#">Softether</a> | <a href="#">Vpn</a> | 5.02      | All    | All     | All      |

## References

| Reference   | Source  | Link  | Tags          |
|---|---------|---|---------------|
| TALOS-2023-1741    Cisco Talos Intelligence Group - Comprehensive Threat Intelligence | MISC    | <a href="https://talosintelligence.com">talosintelligence.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, ar |

No vendor comments have been submitted for this CVE.

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

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)