



CVE-2023-28436

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

Summary

CVE	CVE-2023-28436
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-03-23 20:15:00 UTC
Updated	2023-11-07 04:10:00 UTC
Description	Tailscale is software for using Wireguard and multi-factor authentication (MFA). A vulnerability identified in the implementation of the SSH client.

Risk And Classification

Problem Types: CWE-269

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Tailscale	Tailscale	All	All	All	All

References

Reference
Release 1.38.2 · tailscale/tailscale · GitHub
Non-interactive Tailscale SSH sessions on FreeBSD may use the effective group ID of the tailscaled process · Advisory · tailscale/tailscale · GitHub
ssh/tailssh: fix privilege dropping on FreeBSD; add tests · tailscale/tailscale@d00c046 · GitHub
Security Bulletins · Tailscale
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

691096 Free Berkeley Software Distribution (FreeBSD) Security Update for tailscale (1b15a554-c981-11ed-bb39-901b0e9408dc)

© [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](#)