



CVE-2022-41925

Published on: Not Yet Published

Last Modified on: 12/01/2022 05:10:00 PM UTC

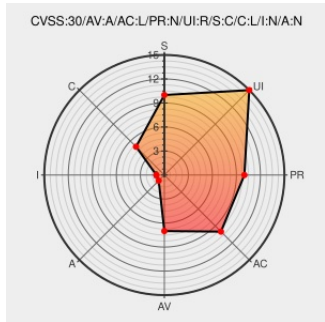
CVE-2022-41925 - advisory for GHSA-qccm-wmcq-pwr6

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Tailscale](#) from [Tailscale](#) contain the following vulnerability:

A vulnerability identified in the Tailscale client allows a malicious website to access the peer API, which can then be used to access Tailscale environment variables. In the Tailscale client, the peer API was vulnerable to DNS rebinding. This allowed an attacker-controlled website visited by the node to rebind DNS for the peer API to an

attacker-controlled DNS server, and then making peer API requests in the client, including accessing the node's Tailscale environment variables. An attacker with access to the peer API on a node could use that access to read the node's environment variables, including any credentials or secrets stored in environment variables. This may include Tailscale authentication keys, which could then be used to add new nodes to the user's tailnet. The peer API access could also be used to learn of other nodes in the tailnet or send files via Taildrop. All Tailscale clients prior to version v1.32.3 are affected. Upgrade to v1.32.3 or later to remediate the issue.

CVE-2022-41925 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: tailscale - tailscale version < 1.32.3

CVSS3 Score: **8.8 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
ADJACENT_NETWORK	LOW	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
CHANGED	HIGH	HIGH	HIGH

CVE References

Description	Tags	Link
CVE-2022-41925: BOF in Tailscale's DNS Rebinding, and You		MICO-00141925@tailscale

CVE-2022-41924 - RCE in Tailscale, DNS Redinding, and you

emily.id.au
[text/html](#)

 emily.id.au/tailscale

Tailscale daemon is vulnerable to information disclosure via CSRF
· Advisory · tailscale/tailscale · GitHub

github.com
[text/html](#)

 CONFIRM
github.com/tailscale/tailscale/security/advisories/GHSA-qccm-wmcq-pwr6

Security Bulletins · Tailscale

tailscale.com
[text/html](#)

 MISC tailscale.com/security-bulletins/#ts-2022-005

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

Related QID Numbers

[690993](#) Free Berkeley Software Distribution (FreeBSD) Security Update for tailscale (e0f26ac5-6a17-11ed-93e7-901b0e9408dc)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Tailscale	Tailscale	All	All	All	All
cpe:2.3:a:tailscale:tailscale:*:*:*:*:*:*						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @OpenBSD_ports	abieber@ modified net/tailscale: Update tailscale to 1.32.3 This includes the fix for CVE-2022-41925 (TS-2022-005).	2022-11-21 20:25:22
 /r/netcve	CVE-2022-41925	2022-11-23 19:38:12

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2022   |

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](#).

CVE.report and Source URL Uptime Status status.cve.report