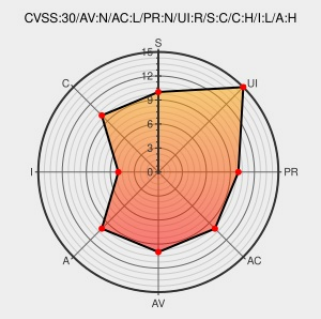
CVE-2022-41924

Published on: Not Yet Published

Last Modified on: 12/01/2022 03:45:00 PM UTC

CVE-2022-41924 - advisory for GHSA-vqp6-rc3h-83cp

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Windows from Microsoft contain the following vulnerability:

A vulnerability identified in the Tailscale Windows client allows a malicious website to reconfigure the Tailscale daemon `tailscaled`, which can then be used to remotely execute code. In the Tailscale Windows client, the local API was bound to a local TCP socket, and communicated with the Windows client GUI in cleartext with no Host header verification. This allowed an attacker-controlled website visited by the node to rebind DNS to an attacker-controlled DNS server, and then make local API requests in the client, including changing the coordination server to an attacker-controlled coordination server. An attacker-controlled coordination server can send malicious URL responses to the client, including pushing executables or installing an SMB share. These allow the attacker to remotely execute code on the node. All Windows clients prior to version v.1.32.3 are affected. If you are running Tailscale on Windows, upgrade to v1.32.3 or later to remediate the issue.

CVE-2022-41924 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as CRITICAL severity.

Affected Vendor/Software: **tailscale** - **tailscale** version **< 1.32.3**

CVSS3 Score: 9.6 - CRITICAL

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

CVE References

Description	Tags	Link
Security Bulletins · Tailscale	tailscale.com	MISC tailscale.com/security-bulletins/#ts-2022-004

	text/html	
CVE-2022-41924 - RCE in Tailscale, DNS Rebinding, and You	emily.id.au text/html	MISC emily.id.au/tailscale
Tailscale Windows daemon is vulnerable to RCE via CSRF · Advisory · tailscale/tailscale · GitHub	github.com text/html	CONFIRM github.com/tailscale/tailscale/security/advisories/GHSA-vqp6-rc3h-83cp

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.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Microsoft	Windows	-	All	All	All
Application	Tailscale	Tailscale	All	All	All	All

cpe:2.3:o:microsoft:windows:-:*:*:*:*:*:*:*:

cpe:2.3:a:tailscale:tailscale:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@hn_frontpage	CVE-2022-41924 – tailscaled can be used to remotely execute code L: tailscale.com/security-bulle… C: news.ycombinator.com/item?id=336958…	2022-11-21 18:23:53
@radoncnotes	CVE-2022-41924 – tailscaled can be used to remotely execute code ift.tt/mCVlSnM 3	2022-11-21 18:25:10
@terrypferguson	CVE-2022-41924 – tailscaled can be used to remotely execute code ift.tt/q2dHaRF 3	2022-11-21 18:28:20
@knelsonvsi	CVE-2022-41924 – tailscaled can be used to remotely execute code ift.tt/qxlwZ9M 3	2022-11-21 18:28:47
@winsontang	CVE-2022-41924 – tailscaled can be used to remotely execute code tailscale.com/security-bulle…	2022-11-21 18:29:03
@HNTweets	CVE-2022-41924 – tailscaled can be used to remotely execute code: tailscale.com/security-bulle… Comments: news.ycombinator.com/item?id=336958…	2022-11-21 18:30:02
@HackerNewsTop10	CVE-2022-41924 – tailscaled can be used to remotely execute code Link: tailscale.com/security-bulle… Comments: news.ycombinator.com/item?id=336958…	2022-11-21 18:32:12
@betterhn20	CVE-2022-41924 – tailscaled can be used to remotely execute code tailscale.com/security-bulle… (news.ycombinator.com/item?id=336958…)	2022-11-21 18:37:30
@betterhn50	CVE-2022-41924 – tailscaled can be used to remotely execute code tailscale.com/security-bulle… (news.ycombinator.com/item?id=336958…)	2022-11-21 19:00:14

@newsycombinator	CVE-2022-41924 – tailscaled can be used to remotely execute code tailscale.com/security-bulle…	2022-11-21 19:00:29
@newsvogueindia	New top story on Hacker News: CVE-2022-41924 – tailscaled can be used to remotely execute code ift.tt/SeIDWo7	2022-11-21 19:00:41
@hackernewsj	CVE-2022-41924 – tailscaled を使用して、Windows でコードをリモートで実行できる tailscale.com/security-bulle…	2022-11-21 19:10:47
@winsontang	CVE-2022-41924 – tailscaled can be used to remotely execute code on Windows emily.id.au/tailscale?utm_…	2022-11-21 19:15:33
@HNTweets	CVE-2022-41924 – tailscaled can be used to remotely execute code on Windows: emily.id.au/tailscale Comments: news.ycombinator.com/item?id=336958…	2022-11-21 19:20:02
@CommentsHn	CVE-2022-41924 – tailscaled can be used to remotely execute code - tailscale.com/security-bulle… 84 points - 27 comments… twitter.com/i/web/status/1…	2022-11-21 19:21:04
@top_hn_bot	New top story! Poster: ghuntley Title: CVE-2022-41924 – tailscaled can be used to remotely execute code on Windows… twitter.com/i/web/status/1…	2022-11-21 19:30:17
@lobsters	CVE-2022-41924 - RCE in Tailscale, DNS Rebinding, and You lobste.rs/s/ypn8zp #security emily.id.au/tailscale	2022-11-21 19:45:09
@newsycombinator	CVE-2022-41924 – tailscaled can be used to remotely execute code on Windows emily.id.au/tailscale	2022-11-21 20:01:13
@ZeroGdoubleD	CVE-2022-41924 - RCE in Tailscale, DNS Rebinding, and You emily.id.au/tailscale	2022-11-21 20:05:01
@CommentsHn	CVE-2022-41924 – tailscaled can be used to remotely execute code on Windows - emily.id.au/tailscale 209 points -… twitter.com/i/web/status/1…	2022-11-21 20:20:50
@suitingtseng	CVE-2022-41924 – tailscaled can be used to remotely execute code on Windows news.ycombinator.com/item?id=336958…	2022-11-21 20:22:51
@newsyc200	CVE-2022-41924 – tailscaled can be used to remotely execute code on Windows emily.id.au/tailscale (news.ycombinator.com/item?id=336958…)	2022-11-21 20:34:04
@newsyc250	CVE-2022-41924 – tailscaled can be used to remotely execute code on Windows emily.id.au/tailscale (news.ycombinator.com/item?id=336958…)	2022-11-21 20:48:35
@markcartertm	? CVE-2022-41924 - RCE in Tailscale, DNS Rebinding, and You - The speed and quality of @Tailscale response to our… twitter.com/i/web/status/1…	2022-11-21 23:03:24
@Komodosec	#security CVE-2022-41924 - RCE in Tailscale, DNS Rebinding, and You emily.id.au/tailscale?utm_…	2022-11-21 23:15:07
@InfoSecSherpa	CVE-2022-41924 - RCE in Tailscale, DNS Rebinding, and You 25 min read Jamie McClymont & Emily Trau 2022-11-22 emily.id.au	2022-11-22 00:48:15
@veritopa_media	New best story on Hacker News: CVE-2022-41924 – tailscaled can be used to remotely execute code on Windows ift.tt/mtp0Vza	2022-11-22 01:21:40
@rakhisharma01	New best story on Hacker News: CVE-2022-41924 – tailscaled can be used to remotely execute code on Windows… twitter.com/i/web/status/1…	2022-11-22 01:35:52
@ali_is_digital	New best story on .@hackernewsbot: CVE-2022-41924 – tailscaled can be used to remotely execute code on Windows ift.tt/2gAfZrw	2022-11-22 01:46:09
@rahul_bahuguna	CVE-2022-41924 – tailscaled can be used to remotely execute code on Windows ift.tt/s95OikM #technews #news	2022-11-22 01:47:15
@BreakTheSec	CVE-2022-41924: Tailscale - Remote code execution vulnerability emily.id.au/tailscale #infosec #vulnerability… twitter.com/i/web/status/1…	2022-11-22 02:05:13
@DavidsonLuna	CVE-2022-41924 – tailscaled can be used to remotely execute code on Windows ift.tt/gIjhpSP #tech #technology #news via Hacker News	2022-11-22 02:08:29

@AlikKarmokar	New best story on Hacker News: CVE-2022-41924 – tailscaled can be used to remotely execute code on Windows ift.tt/j68V4zY	2022-11-22 02:12:25
@Tsuki_	CVE-2022-41924 - RCE in Tailscale, DNS Rebinding, and You ift.tt/tN4q1lY	2022-11-22 02:13:27
@newsycombinator	CVE-2022-41924 – tailscaled can be used to remotely execute code on Windows emily.id.au/tailscale	2022-11-22 03:00:28
@Linda_pp	Tailscale にリモートコード実行の脆弱性が出てる（CVE-2022-41924）．昨日のリリースにアップデートが必要 emily.id.au/tailscale	2022-11-22 03:16:02
@CommentsHn	CVE-2022-41924 – tailscaled can be used to remotely execute code on Windows - emily.id.au/tailscale 577 points -… twitter.com/i/web/status/1…	2022-11-22 03:20:51
@ens7piper	New best story on Hacker News: CVE-2022-41924 – tailscaled can be used to remotely execute code on Windows bit.ly/3GAGExd	2022-11-22 04:00:00
@Din3zh	CVE-2022-41924 - RCE in Tailscale, DNS Rebinding, and You - emily.id.au/tailscale #RCE #CVE	2022-11-22 04:20:20
@kdmsnr	CVE-2022-41924 – tailscaled を使用して、Windows でコードをリモートで実行できる via Hacker News ift.tt/1bYkmDn	2022-11-22 05:04:47
@omiossec_med	CVE-2022-41924 - RCE in Tailscale, DNS Rebinding, and You emily.id.au/tailscale	2022-11-22 05:44:50
@GavLaaaaaaaa	CVE-2022-41924 - RCE in Tailscale, DNS Rebinding, and You emily.id.au/tailscale #programming #softwareengineering… twitter.com/i/web/status/1…	2022-11-22 06:42:33
@SproutCats	CAT HACKER: CVE-2022-41924 – tailscaled can be used to remotely execute code on Windows bit.ly/3V10N4e	2022-11-22 06:45:57
@sharon_smith_1	CVE-2022-41924 – tailscaled can be used to remotely execute code on Windows bit.ly/3V10N4e	2022-11-22 06:49:47
@Cloud_Devops	CVE-2022-41924 – tailscaled can be used to remotely execute code on Windows emily.id.au/tailscale	2022-11-22 07:10:00
@gaetanoz	CVE-2022-41924 - RCE in Tailscale, DNS Rebinding, and You emily.id.au/tailscale	2022-11-22 07:48:37
@n0ipr0cs	CVE-2022-41924 - RCE in Tailscale, DNS Rebinding, and You emily.id.au/tailscale	2022-11-22 13:40:32
@CVEtrends	Top 3 trending CVEs on Twitter Past 24 hrs: CVE-2022-41924: 954.6K (audience size) CVE-2022-41040: 454.4K CVE-2022… twitter.com/i/web/status/1…	2022-11-22 14:00:04
@Har_sia	CVE-2022-41924 har-sia.info/CVE-2022-41924… #HarsiaInfo	2022-11-22 15:07:45
@Har_sia	CVE-2022-41924 har-sia.info/CVE-2022-41924… #HarsiaInfo	2022-11-22 18:23:34
@GeekNewsBot	CVE-2022-41924 - Tailscale news.hada.io/topic?id=7877 - Tailscale - … twitter.com/i/web/status/1…	2022-11-23 03:11:03
@IT_CORD	#GeekNews # CVE-2022-41924 - Tailscale news.hada.io/topic?id=7877 #IT #TECH # #Trends #	2022-11-23 04:04:32
@matsuu_zatsu	CVE-2022-41924 – tailscaled can be used to remotely execute code tailscale.com/security-bulle…	2022-11-23 05:35:49
@pinboard_pop	CVE-2022-41924 - RCE in Tailscale, DNS Rebinding, and You emily.id.au/tailscale	2022-11-23 08:00:05
@ChrisShort	Suggested Read: CVE-2022-41924 - RCE in Tailscale, DNS Rebinding, and You emily.id.au/tailscale	2022-11-23 13:47:01

	emily.id.au/tailscale	13:47:01
/r/cybersecurity	CVE-2022-41924 - RCE in Tailscale, DNS Rebinding, and You	2022-11-21 18:32:38
/r/programming	CVE-2022-41924 - RCE in Tailscale, DNS Rebinding, and You	2022-11-21 18:29:27
/r/Tailscale	CVE-2022-41924 - Tailscale, DNS Rebinding, and You	2022-11-21 18:27:10
/r/hypeurls	CVE-2022-41924 – tailscaled can be used to remotely execute code	2022-11-21 19:06:34
/r/patient_hackernews	CVE-2022-41924 – tailscaled can be used to remotely execute code on Windows	2022-11-21 20:46:30
/r/devopsish	CVE-2022-41924 - RCE in Tailscale, DNS Rebinding, and You	2022-11-21 20:34:24
/r/fastvoted	Hacker News: CVE-2022-41924 – tailscaled can be used to remotely execute code on Windows | 165 points in 2 hours	2022-11-21 20:02:07
/r/hackernews	CVE-2022-41924 – tailscaled can be used to remotely execute code on Windows	2022-11-21 20:00:03
/r/netcve	CVE-2022-41924	2022-11-23 19:38:13

← 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 registred 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