Security Bulletins

Security notifications affecting the Tailscale client and service

If you're directly affected by a security issue in Tailscale, and we have your contact information, we will contact you.

Subscribe via RSS Follow on Twitter Report a vulnerability

Jan 17, 2023

TS-2023-001

Description: An issue in the Tailscale coordination server allowed a malicious individual to share nodes from other tailnets to themselves, if they knew the node ID of the target.

What happened?

A bug in Tailscale's node sharing logic allowed the creation of sharing invitations by unauthorized users. A malicious individual who knew a target node's database ID could generate and accept a sharing invite for that node without being an admin of the target node's tailnet.

This was possible for any node in any tailnet, as long as the individual knew the target's node ID. The node ID is an integer used in the admin panel's database, and is not related to the node "StableID" that is visible to Tailscale clients. A node's ID is only visible in the API or admin console, by admins of either the node's tailnet or a tailnet to which that node has already been shared. IDs are random 64-bit numbers that are not sequential or otherwise easily guessable.

The bug was introduced on 2022-09-14, reported to us on 2023-01-11, and remediated on 2023-01-12.

Who is affected?

All tailnets with nodes are affected.

What is the impact?

This vulnerability was not triggered or exploited. Analysis of tailnet logs shows that no unauthorized shares were created or accepted while the vulnerability was present, except as part of the proof of concept from the individual who reported the vulnerability.

Admins of a tailnet can review nodes that are shared out of their tailnet in the admin console. Sharing invites are logged as events in configuration audit logs. Admins can also review invites created and accepted in their configuration audit logs in the admin console.

What do I need to do?

No action is required. Tailscale has deployed a fix to the coordination server as of 2023-01-12, and verified that the vulnerability was not exploited.

Credits

We would like to thank Benjamin Roberts (tsujamin) for reporting this issue.

Nov 21, 2022

TS-2022-005

Reference: CVE-2022-41925

Severity: Low

CVSS vector string: CVSS:3.0/AV:A/AC:L/PR:N/UI:R/S:C/C:L/I:N/A:N

Description: 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.

Affected platforms: All

Patched Tailscale client versions: v1.32.3 or later, v1.33.257 or later (unstable)

What happened?

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.

Who is affected?

All Tailscale clients prior to version v1.32.3 are affected.

What is the impact?

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.

An attacker with access to the peer API who sent a malicious file via Taildrop which was accessed while it was loading could use this to gain access to the local API, and remotely execute code.

There is no evidence of this vulnerability being purposefully triggered or exploited.

What do I need to do?

Upgrade to v1.32.3 or later to remediate the issue.

Credits

We would like to thank Emily Trau and Jamie McClymont (CyberCX) for reporting this issue. Further detail is available in their blog post.

Nov 21, 2022

TS-2022-004

Reference: CVE-2022-41924

Severity: Critical

CVSS vector string: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:H

Description: 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.

Affected platforms: Windows

Patched Tailscale client versions: v1.32.3 or later, v1.33.257 or later (unstable)

What happened?

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.

Who is affected?

All Windows clients prior to version v1.32.3 are affected.

What is the impact?

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.

Reviewing all logs confirms this vulnerability was not triggered or exploited.

What do I need to do?

If you are running Tailscale on Windows, upgrade to v1.32.3 or later to remediate the issue.

Credits

We would like to thank Emily Trau and Jamie McClymont (CyberCX) for reporting this issue. Further detail is available in their blog post.

Jun 14, 2022

TS-2022-003

Description: An issue in Tailscale's implementation of the OAuth authentication flow for GitHub allowed users who authenticate to Tailscale with their GitHub user identity to create a tailnet for a GitHub organization using SAML

authentication in GitHub Enterprise Cloud, where Tailscale is not an authorized OAuth app for their organization.

What happened?

Tailscale silently ignored a 403 error to the GitHub API query for organizations for an authenticated user that was returned when a user authenticated to SAML, but the organization had not authorized Tailscale. This only applied to organizations using SAML on GitHub Enterprise Cloud with OAuth app authorization enabled, and where Tailscale was not authorized.

As a result, a user identity could bypass the organization's OAuth app access restrictions, and create a tailnet for the GitHub organization.

Who is affected?

Up to 7 tailnets for GitHub organizations on GitHub Enterprise Cloud which use SAML for authentication may have been created between 2021-06-18 and 2022-06-03 without Tailscale being an authorized OAuth app for their GitHub organization, and could have used Tailscale to connect devices in that organization. An additional 10 tailnets were created with no or only one device, and so could not have used Tailscale to connect between devices.

We have notified the Tailscale admins for the affected organizations who we were able to identify. We do not have a way to notify the GitHub organization owners.

If you're a GitHub organization owner, you can see if Tailscale is approved for your GitHub organization by going to the organization's settings page and selecting "Third-party access" from the left-hand navigation. Or, for an organization `$your-org`, navigate to

```
https://github.com/organizations/$your-org/settings/oauth_application_policy
```

What is the impact?

A tailnet may have been created for a GitHub organization without their GitHub organization owner's approval. In this case, the use of Tailscale and the creation of a tailnet could be perceived as being sanctioned by their organization when it might not have been.

What do I need to do?

If you are affected, you will need to re-authenticate to keep using your tailnet. Tailscale has expired all admin console sessions for potentially affected GitHub organizations as of 2022-06-13. As a result, users in a potentially affected tailnet will need to re-authenticate the next time they access the admin console, and will not be able to do so without Tailscale being an authorized OAuth app, which may first require getting approval from their GitHub organization owner. Nodes in a potentially affected tailnet will also need to re-authenticate when their node keys expire. If you're a GitHub organization owner, you can approve Tailscale as an OAuth app by following GitHub's instructions for Approving OAuth Apps for your organization.

Tailscale has deployed a fix to the coordination server as of 2022-06-03, so that no new tailnets can be created without a GitHub organization owner's approval.

Credits

We would like to thank Aurelia for reporting the issue. Further detail is available in their blog post.

May 11, 2022

TS-2022-002

Description: An issue in the Tailscale coordination server allowed individuals creating a new Tailscale account with a gmail.com email address to join the same tailnet, rather than individual tailnets.

What happened?

There was a flaw in Tailscale's logic for migrating accounts between identity providers, and a new gmail.com shared tailnet was accidentally created. Once created, any user who tried to create a new Tailscale account with a gmail.com email address joined the shared gmail.com tailnet.

Who is affected?

A total of 44 users with 59 devices who created accounts for their gmail.com email addresses on 2022-05-11 between 10:56 and 13:12 PT were affected. We have notified affected users.

What is the impact?

Six connections between devices belonging to different users were made, but no traffic of concern flowed between them. Four connections were pings, and two connections were UDP traffic on port 27036, likely automated broadcasting by a gaming platform to discover peers to play with. There is no evidence of malicious traffic.

Impacted users could see some metadata about other users and devices from their devices' clients, including users' names, devices' host names, and devices' Tailscale IP addresses. This information *was* viewed by at least one user, who reported it to us.

One user, the tailnet Admin, was able to see all users and devices added to the shared gmail.com tailnet. This includes users' email addresses, names, and when they were last connected; and devices' host names, their OS and version, when the devices were last connected, and their public IP addresses. This information *was* viewed by the user, who reported it to us.

What do I need to do?

No action is required. Tailscale has deployed a fix to the coordination server as of 2022-05-11 13:12 PT.

New users registering for a Tailscale account with a gmail.com email address will create a single-user tailnet as normal.

Credits

We would like to thank David Swafford and George Constantinides for reporting the issue.

Feb 7, 2022

TS-2022-001

Description: An issue in the Tailscale coordination server allowed individuals using GitHub to authenticate to Tailscale to have their devices join a tailnet associated with an empty GitHub username.

What happened?

There was a flaw in Tailscale's authorization logic for the GitHub identity provider. If a user tried to authenticate to Tailscale using their GitHub identity, and GitHub returned a 500 error, then in some cases, Tailscale interpreted that as authorization for an empty GitHub username, and connected these devices to the tailnet associated with the empty GitHub username.

Who is affected?

A total of five devices belonging to four users were affected between 2021-06-15 and 2022-02-04, when the issue was reported and remediated. We have contacted the two users we were able to identify.

You may be affected if you authenticated to Tailscale using a GitHub account, and after authorizing a connection using GitHub, you received a connection error. Without being asked to select which GitHub user or organization tailnet to connect to, your device would have connected to a tailnet.

What is the impact?

No device connected to another device in the tailnet. Other than the two devices which belonged to the same user, no two devices in the tailnet had valid node keys at the same time, and so did not and would not have been able to establish connections.

A device's existence and some metadata was shared with devices added later in time. Devices added later in time were able to see previously added devices, including: their host names, their OS and version, when the devices were last connected, and their public IP addresses.

There is no evidence of this vulnerability being purposefully triggered or exploited.

Credits

We would like to thank Marvin Boothby (boothb) for reporting the issue.

tailscale

Privacy & Terms