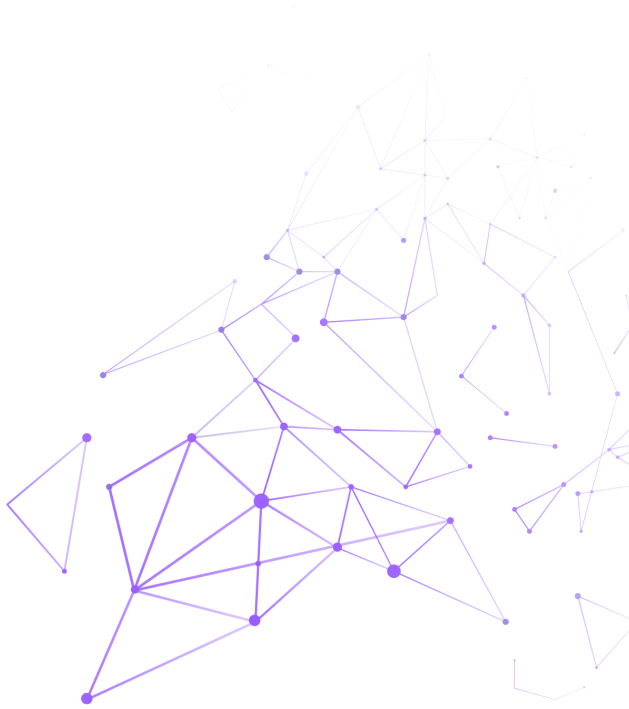
Teleport



Root Cause Analysis

CVE-2025-49825 Root Cause Analysis

Teleport

Summary

On June 5, 2025, our engineers discovered a critical severity vulnerability in Teleport. CVE-2025-49825 is a remote authentication bypass due to a bug in SSH certificate validation logic within Teleport.

The security vulnerability was introduced in Teleport in 37ab159. In this commit, the user and host authority validation logic was updated to add a type assertion to handle a special case: validating that an SSH host certificate presented by an upstream server was issued by a Teleport CA. The root cause of the vulnerability is that the logic unnecessarily accepts an SSH certificate as a valid signer, where only CA keys should be accepted. On its own, this logic would not create a vulnerability. However it coincided with an issue in x/crypto/ssh that allowed `IsUserAuthority` and `IsHostAuthority` to be passed certificates as CA keys and became a critical severity vulnerability. The combined logic could have allowed an SSH certificate to bypass remote authentication verification by signing a forged certificate with another certificate instead of a CA key.

Due to the critical nature of the vulnerability, the Teleport team added two additional weeks to our normal one-week customer-only embargo to give open source users time to update their infrastructure before we published this report. Additionally, for these specific patch versions of Teleport Community Edition, we removed Community Edition restrictions on employee count or revenue thresholds to prioritize community safety.

Timeline

May 30, 2025
One of Teleport's engineers noticed an unnecessary type assertion made by the Teleport codebase in a callback function, which is called from the `x/crypto/ssh` package. A message was sent to the maintainers of `x/crypto/ssh` to confirm the engineer's understanding that calling this function with anything other than `ssh.PublicKey` is a violation of the specification. At this point, the code in question appeared to be unreachable code instead of a security vulnerability.

June 2, 2025
The maintainers of `x/crypto/ssh` replied that this was indeed a specification violation and they would create a fix for `x/crypto/ssh`. In discussing the issue with the maintainers of `x/crypto/ssh`, both teams concluded that this wasn't a security concern.

June 4, 2025
The maintainers of `x/crypto/ssh` created CL 678716 to fix the issue.

Teleport

June 5, 2025
While reviewing the patch to `x/crypto/ssh`, our engineering team identified that the code in question could be a security vulnerability and spent time investigating if this code path could be exploited.

June 5, 2025
Once it became clear this was a security vulnerability, we initiated our Security Incident Response Plan. Members of our security and engineering teams reviewed and confirmed the severity of the problem, and sent instructions to internal teams to prioritize patching the issue, and delay/pause any other work streams. The remainder of the day was spent working on the patch.

June 6, 2025
A PR with a fix for the security vulnerability was raised, and approximately two hours later, fixes were backported to all supported releases: Teleport 17, 16, and 15. Due to the severity of this issue, we spent several days backporting fixes to EOL releases of Teleport 14, 13, 12, 11, and 10. By the end of the day, we began sending out notifications to customers that a critical security vulnerability existed in Teleport, patches were available, and we offered hands-on support to help all customers update as quickly as possible. At this point, a one week customer-only embargo was initiated.

June 7, 2025
We began patching Cloud customer control planes. Under normal conditions, patching occurs over a 24-hour period during the customer's scheduled upgrade window. In this case, we decided to override all upgrade windows and update all customers immediately. By the end of the day, all Cloud customer control planes had been patched, reducing the issue from an unauthenticated remote code execution vulnerability to a privilege escalation vulnerability for customers who haven't yet upgraded their SSH nodes.

In parallel, we engaged an external security research firm Doyensec to audit the fixes to ensure that it fully patched the issue and to look for similar patterns within the code base that may have been missed by internal reviews. This analysis continued through June 13, concluding that no patterns allowing for similar exploits were identified. Doyensec's full report is included at the end of this document.

June 8, 2025
Cloud agent upgrades were initiated for customers enrolled in Managed Updates. All agents enrolled in Managed Updates were updated within 24 hours, depending on their selected update window.

June 9, 2025

Teleport

We initiated a targeted customer outreach program to confirm acknowledgement of our notification from all customers by the end of the customer-only embargo period and support them in upgrading their instances of Teleport.

At this point and under normal circumstances, the patch for the security vulnerability would be merged into the public Teleport repo. However, due to the critical nature of this vulnerability, we extended the embargo by two weeks to allow open source users to upgrade.

June 16, 2025
The two-week open source embargo phase began, during which time we publicly disclosed CVE-2025-49825, but kept the details of the vulnerability private to give open source users time to upgrade. We also updated the license for Teleport Community Edition to remove restrictions for specific patched versions on employee count or revenue thresholds as long as the patch was applied within 30 days of its official release.

In parallel, we engaged with Wiz and Project Discovery to ensure CVE-2025-49825 was incorporated into CVE scanners to reach a broader audience and help update more Teleport users.

We collaborated with Project Discovery to identify servers running vulnerable versions of Teleport using internet scanning data, allowing us to conduct direct outreach to the associated companies.

June 17, 2025
We released an Indicator of Compromise (IOC) tool for customers to run against their Audit Log.

June 20, 2025
During a secondary review of the incident, we discovered that our FIPS builds running in FIPS mode (using the `--fips` flag) were not vulnerable to this issue.

June 30, 2025
CL 678716 to fix the issue in Go `x/crypto/ssh` was merged.

Impact

This issue impacted Teleport SSH agents, OpenSSH integration, and git integration. The severity was reduced in cases where Teleport Proxies and SSH agents were not accessible outside of the customer's network perimeter.

As of the time of this report, based on our audit log scan, no Cloud customers were impacted. No self-hosted customers have reported being impacted after running the IOC tool.

The following were not affected:

- Teleport Cloud Infrastructure and CI/CD build, test, and release infrastructure Teleport infrastructure that hosts customer data
- Teleport agents for Kubernetes, Databases, Applications, and Windows Desktops

Action Items

We are taking the following steps in response to this incident.

1. We will perform another round of deep auditing in our authentication layer before the end of this year.
2. We are adding multiple layers of defense against authentication vulnerabilities at the transport/protocol layer. Possession of a valid certificate (and private key) will not be enough to compromise Teleport.
3. We will continue to invest in and expand maintenance of dependencies we use through Geomys, Doyensec, and other firms.
4. We will increase our investment in public audits of our open source dependencies.
5. We will improve our customer communication system to make sure all customer contacts are up to date and can receive and acknowledge critical notifications.

Doyensec LLC
350 Townsend Street, Suite 840
94107 San Francisco
California, United States

Vulnerability Analysis Overview

On 06/05/2025, an internal security review found that an issue with Go's `crypto`[1] library, combined with mishandling of SSH certificate signature keys allowed for a full bypass of Teleport's authentication and authorization controls, and lead to unauthorized access to SSH resources.

Doyensec was approached to perform a review of Teleport's implementation of SSH servers to ensure that similar issues do not exist. The review commenced on 06/09/2025 and ended on 06/13/2025.

Individual steps of Doyensec's approach are outlined below.

Understanding and Reproducing the Vulnerability

The review started with an analysis of commits, both on the Go `crypto` library, and Teleport's application code, all supplied by Teleport engineers. This allowed Doyensec to perform static analysis and helped in understanding the root cause of the vulnerability.

The results of the static analysis were augmented by verifying the proof-of-concept (PoC) script provided by Teleport on a self-managed cluster, as well as replicating the vulnerable code pattern locally, which provided a flexible environment to instrument and inspect individual parts of the execution flow.

This methodology proved invaluable in providing a complete understanding of the issue and how to exploit it.

In summary, the issue revolves around:

1. A bug in Go's `crypto` library, that allowed creation and parsing of SSH certificates that have another SSH certificate set as a signature key, which is against the specification
2. A mishandling of that particular case in the Teleport code, which performed validation on data from a certificate signature key without verifying its signature, allowing for a bypass of the public key verification step

The combination of these two issues ultimately allowed for an attacker to create a user SSH certificate, signed by another certificate which points to a legitimate Teleport CA public key. Connection attempts with the user certificate were accepted by Teleport, granting the user access to the target resource.

[1] https://github.com/golang/crypto

Doyensec LLC
350 Townsend Street, Suite 840
94107 San Francisco
California, United States

Application Code Review

After understanding the vulnerability and how to reproduce it, Doyensec shifted focus on reviewing all SSH servers implemented and used throughout Teleport to provide users access to Teleport-protected resources.

The review focused on the following:

- Similar patterns of incorrectly handling SSH certificate signature keys
- User SSH certificate handling and validation
- Host SSH certificate handling and validation
- General misconfigurations of SSH servers

The vulnerable functions `authorityForCert` and `makeIsHostAuthorityFunc` were found to be reachable when authenticating to the SSH servers listed below.

- `teleport/lib/srv/regular/sshserver.go`
- `teleport/lib/srv/git/forward.go`

In all cases, the vulnerable function is called by the `PublicKeyCallback` callback function, that is invoked by the SSH server on all incoming client connections.

No other issues or misconfigurations were identified in Teleport's implementation of SSH servers.

Patch Analysis

As a final step, Doyensec performed a review of the patches of both Teleport code and Go's `crypto` library, attempting to find bypasses of the implemented mitigations.

Summary

The review outlined in this document aimed at analyzing the vulnerability discovered by the Teleport team, and finding similar patterns that may open up the system to further exploitation.

Doyensec believes that all patches introduced are robust and provide the necessary security controls to protect against the behaviors that ultimately led to the vulnerability.