







[G...](#)
CHANGES ▾
DOCUMENTATION ▾
BROWSE ▾
Search
Sign in

Merged [737700](#) crypto/tls: check verifiedChains roots when resuming ses Loading actions...

### Change Info

Show All ▾

Sign in

Submitted Jan 28  
 Owner  Roland Shoemaker  
 Uploader  Gopher Robot  
 Reviewers  Filippo Valsor... +2  
                   Dmitri Shuraly... +1 Deleted User +1  
                   Gopher Robot  Go LUCI  
 CC  Dmitri Shuraly...  
 Repo | [go](#) | [master](#)  
 Branch

crypto/tls: check verifiedChains roots when res

When resuming TLS sessions, on the server and c chains stored in the session state (verifiedCha with regards to the Config by checking for the either ClientCAs (server) or RootCAs (client). a session with a certificate chain that would b handshake due to an untrusted root.

Updates [#77113](#)  
 Updates [#77217](#)  
 Updates CVE-2025-68121

Change-Id: [I11fe00909ef1961c24ecf80bf5b97f7b112](#)  
 Reviewed-on: <https://go-review.googlesource.com>  
 Auto-Submit: Roland Shoemaker <[roland@golang.org](mailto:roland@golang.org)>

[Show All](#)

### Submit Requirements

- Code-Review +2 +1
- No-Unresolved-Comments Satisfied
- Review-Enforcement Satisfied
- TryBots-Pass +1

### Trigger Votes

Auto-Submit +1

Comments 30 resolved

Checks Loading results







Files      Comments      Checks

Base ▾ → Patchset 10 ▾  [026fa9d](#) Download Expand All



File	C	Delta
------	---	-------

### Change Log



Show all entries (32 hidden) Expand All

-  Roland Shoemaker Uploaded patch set 1. View Diff Patchset 1 | Jan 20 9:36 PM ▾
-  Roland Shoemaker Commit-Queue +1 This change is ready for review. Patchset 1 | Jan 21 7:02 PM ▾
-  Roland Shoemaker 1 Patchset 1 | Jan 21 7:02 PM ▾
-  Filippo Valsorda 4 I think this is regressing the InsecureSkipVerify / lower Cl... Patchset 1 | Jan 21 7:14 PM ▾
-  Roland Shoemaker 1 I meant to leave a note about this. When I was looking a... Patchset 1 | Jan 21 7:22 PM ▾
-  Go LUCI This CL has passed the run Patchset 1 | Jan 21 7:42 PM ▾




-  Deleted User  1 Patchset 4 | Jan 26 7:30 PM ▾



---

-  Roland Shoemaker  1 Patchset 5 | Jan 26 7:35 PM ▾


---

-  Roland Shoemaker Commit-Queue +1 Patchset 5 | Jan 26 7:35 PM ▾



---

-  Deleted User  1 Patchset 5 | Jan 26 7:38 PM ▾


---

-  Roland Shoemaker Commit-Queue +1 Patchset 6 | Jan 26 7:39 PM ▾



---

-  Deleted User  1 Patchset 5 | Jan 26 7:39 PM ▾



---

-  Go LUCI This CL has passed the run Patchset 6 | Jan 26 8:04 PM ▾



---

-  Deleted User  1 Patchset 6 | Jan 26 8:09 PM ▾



---

-  Filippo Valsorda  5 Patchset 6 | Jan 27 6:48 PM ▾


---

-  Deleted User  1 Patchset 6 | Jan 27 7:17 PM ▾



---

-  Roland Shoemaker  5 Patchset 7 | Jan 27 7:32 PM ▾



---

-  Roland Shoemaker Commit-Queue +1 Patchset 7 | Jan 27 7:33 PM ▾



---

-  Deleted User  2 Patchset 7 | Jan 27 7:38 PM ▾


---

-  Deleted User  1 Patchset 7 | Jan 27 7:41 PM ▾



---

-  Roland Shoemaker  3 Patchset 8 | Jan 27 7:48 PM ▾


---

-  Roland Shoemaker Commit-Queue +1 Patchset 8 | Jan 27 7:48 PM ▾



---

-  Deleted User Code-Review +1  1 It looks fine, but honestly, reading yo... Patchset 8 | Jan 27 7:57 PM ▾



---

-  Go LUCI This CL has passed the run Patchset 8 | Jan 27 8:14 PM ▾



---

-  Filippo Valsorda  1 Coia, this behavior is not acceptable, no matter what. I wi... Patchset 8 | Jan 27 8:22 PM ▾



---

-  Deleted User  1 I'm sorry for that, but ... I think I'm tell the truth, look at th... Patchset 8 | Jan 27 8:34 PM ▾


---

-  Deleted User  1 Regarding my last point, I think this might be due to cultu... Patchset 8 | Jan 27 8:39 PM ▾



---

-  Filippo Valsorda Code-Review +2  2 Patchset 8 | Jan 27 11:09 PM ▾


---

-  Roland Shoemaker Uploaded patch set 9. Copied Votes: \* Code-Revi... [View Diff](#) Patchset 9 | Jan 28 1:03 AM ▾


---

-  Roland Shoemaker  2 Patchset 9 | Jan 28 1:03 AM ▾



---


















-  Roland Shoemaker Auto-Submit +1 Commit-Queue +1 Patchset 9 | Jan 28 1:03 AM ▾

---

-  Go LUCI Dry run: CV is trying the patch. Bot data: {"action": "start", "trigger... Patchset 9 | Jan 28 1:03 AM ▾

---

-  golang-scoped@luci-project-accounts.iam.gserviceaccount.com on behalf of  Rolan Patchset 9 | Jan 28 1:30 AM ▾

-  **Go LUCI** This CL has passed the run Patchset 9 | Jan 28 1:30 AM 
-  **Go LUCI** LUCI-TryBot-Result +1 Patchset 9 | Jan 28 1:30 AM 
-  **Dmitri Shuralyov** Added to cc:  Dmitri Shuralyov Added to reviewer:  Dmitri Shuralyov Patchset 9 | Jan 28 1:36 PM 
-  **Dmitri Shuralyov** Code-Review +1 Patchset 9 | Jan 28 1:36 PM 
-  **Gopher Robot** Added to reviewer:  Gopher Robot Patchset 9 | Jan 28 4:15 PM 
-  **Gopher Robot** Change has been successfully cherry-picked as ... [View Diff](#) Patchset 10 | Jan 28 4:15 PM 
-  **Deleted User**  1 I had a nightmare after you mentioned the CoC violation... Patchset 10 | Jan 28 4:22 PM 