Merged 737700 crypto/tls: check verifiedChains roots when resuming sessions

Change Info

Show All

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 | Branch go | master

Submit Requirements

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

Trigger Votes

Auto-Submit +1

Sign in

```
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.or
```

Show All

Comments 30 resolved

Checks Loading results

Files | Comments | Checks

Base → Patchset 10 026fa9d Download Expand All

	File	C	Delta
	Commit message		
M	.../common.go		-5 +20
M	.../handshake_client.go		-1 +6
M	.../handshake_server.go		-1 +6
M	.../handshake_server_test.go		-0 +214
M	.../handshake_server_tls13.go		-1 +7
			-8 +253

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
Roland Shoemaker	3		Patchset 2 | Jan 23 7:10 PM
Roland Shoemaker	Commit-Queue +1	2 Switched back to the old behavio…	Patchset 2 | Jan 23 7:11 PM
Deleted User	1		Patchset 2 | Jan 23 7:16 PM
Deleted User	1	and why not directly use https://go-review.googlesource.…	Patchset 2 | Jan 23 7:18 PM
Deleted User	1	Directly cherry-picked it are okay,commit message see Gi…	Patchset 2 | Jan 23 7:24 PM
Deleted User	1	Now is 03:24 AM in China and I can wait for all thing don…	Patchset 2 | Jan 23 7:26 PM
Roland Shoemaker	2	CL 737200 is a significantly broader change. For these t…	Patchset 3 | Jan 23 7:33 PM
Roland Shoemaker	Commit-Queue +1		Patchset 3 | Jan 23 7:33 PM
Deleted User	1	Expectations¶ Although we expect that the vast majority …	Patchset 3 | Jan 23 7:35 PM
Deleted User	1	And I said, you can delete some for that CL. Because so…	Patchset 3 | Jan 23 7:37 PM
Deleted User	2	If you clearly understand how the user uses that callback…	Patchset 3 | Jan 23 7:43 PM
Deleted User	1	Done	Patchset 3 | Jan 23 7:43 PM
Go LUCI		This CL has passed the run	Patchset 3 | Jan 23 8:01 PM
Deleted User	1	In most cases, that CL will not cause any problems; if Ver…	Patchset 3 | Jan 23 8:07 PM
Deleted User	1	A VerifyPeerCertificate usage at https://github.com/gravi…	Patchset 3 | Jan 23 8:20 PM
Deleted User	1	See https://github.com/golang/go/issues/77217#issuec…	Patchset 3 | Jan 23 8:33 PM
Deleted User	1	I provided a new CL for identity freshness only. See https:…	Patchset 3 | Jan 23 9:20 PM
Filippo Valsorda	8	As I asked on #77217, please _please_ open separate G…	Patchset 3 | Jan 23 10:05 PM
Deleted User	1	I have a new CL 738761. I think all issue are reported in …	Patchset 3 | Jan 23 10:19 PM
Filippo Valsorda	1	We have not told you "Works as Intended" on almost an…	Patchset 3 | Jan 23 10:35 PM
Deleted User	1	I understand how you feel. I'm just stating the facts. Ple…	Patchset 3 | Jan 23 10:44 PM
Deleted User	4		Patchset 3 | Jan 24 12:50 AM

Deleted User	1		Patchset 3 | Jan 24 12:25 PM
Filippo Valsorda	2	> Please understand that my tone is due to Linus Torval…	Patchset 3 | Jan 24 12:48 PM
Deleted User	2	I think this is the result of me and Roland being cold ha…	Patchset 3 | Jan 24 12:54 PM
Roland Shoemaker	9		Patchset 4 | Jan 26 7:22 PM
Roland Shoemaker	Commit-Queue +1		Patchset 4 | Jan 26 7:22 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 Rolar		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 S	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