crypto/tls: randomly generate ticket_age_add [freeze exception] #52814

Closed nervuri opened this issue on May 10 · 15 comments

Labels NeedsFix Security

Milestone Go1.19

nervuri commented on May 10 • edited

crypto/tls always sets `newSessionTicketMsgTLS13.ageAdd` to 0, which makes it so that clients resuming a session can't obfuscate the `obfusacted_ticket_age`. This violates the TLS 1.3 spec (RFC 8446, section 4.6.1):

> ticket_age_add: A securely generated, random 32-bit value that is used to obscure the age of the ticket that the client includes in the "pre_shared_key" extension. The client-side ticket age is added to this value modulo 2^32 to obtain the value that is transmitted by the client. **The server MUST generate a fresh value for each ticket it sends.**

See the sendSessionTickets() function.

How to reproduce

- Run a simple TLS server: https://go.dev/play/p/t2moO8mDTmb (notice I set `srv.SetKeepAlivesEnabled(false)` ; we don't want connection reuse)
- open Wireshark, listen on loopback interface and filter on `tls.handshake`
- `curl -k https://localhost:8443 https://localhost:8443`

In Wireshark, open the second Client Hello message, look at the `pre_shared_key` extension and you'll see that `obfuscated_ticket_age` is 0 (or very close to 0).

Proposed fix

Given that you don't check the obfuscated_ticket_age, it's enough to assign `ageAdd` a random value each time.

👍 1

seankhliao added the **NeedsInvestigation** label on May 10

seankhliao commented on May 10 Member

cc **@golang/security**

FiloSottile commented on May 10 Contributor

Ah, yes, that's an oversight, thank you.

I would argue this is worth a freeze exception, because the fix is very simple, we are early in the freeze, and it fixes a privacy issue (allowing network observers to correlate successive connections even if the client changed location). Maybe even worth a CVE and a backport? Not sure. /cc **@golang/release**

If we ever expose the session ticket structure (which might be something that happens as part of #25351 #46718 #19199 #6379), we might want to add the obfuscated_ticket_age to it (or start generating it from the key material?) in case other implementations want to use it, but for now we are the only consumers of the tickets and indeed don't care about it.

(While at it, let's also add a note about why ticket_nonce is always zero, which is simply that we only ever send one ticket. It's a good comment to have in there in case that invariant ever changes.)

👍 1

FiloSottile changed the title ~~crypto/tls: ticket_age_add is always 0~~ **crypto/tls: randomly generate ticket_age_add [freeze exception]** on May 10

nervuri commented on May 10 Author

Here's my patch, for what it's worth:

https://github.com/nervuri/go/commit/1cfb6b392b1d22127c9f6afcf45619d190ed9bfe

Not sure if I should submit it as a pull request... for such a small change, the contribution setup is a tad overkill. :) And you may want to write the patch differently. What do you think?

heschi commented on May 10 Contributor

cc **@golang/security**

If the fix is easy and we can get a CL in before the end of the week I think it's fine. Up to the security team to decide about a CVE/backport.

👍 1

rolandshoemaker commented on May 10 Member

We will work to get a CL in this week. Backporting seems reasonable given how small the fix is.

@gopherbot Please open backport issues for Go 1.17 and Go 1.18, this is a privacy issue.

This was referenced on May 10

crypto/tls: randomly generate ticket_age_add [1.17 backport] #52832

Closed

crypto/tls: randomly generate ticket_age_add [1.18 backport] #52833

Closed

gopherbot commented on May 10

Backport issue(s) opened: #52832 (for 1.17), #52833 (for 1.18).

Remember to create the cherry-pick CL(s) as soon as the patch is submitted to master, according to https://go.dev/wiki/MinorReleases.

komuw commented on May 11 Contributor

> Not sure if I should submit it as a pull request..., the contribution setup is a tad overkill

The Go project does accept normal github pull requests: https://go.dev/doc/contribute#sending_a_change_github

nervuri mentioned this issue on May 11

crypto/tls: randomly generate ticket_age_add #52850

Closed

nervuri commented on May 11 Author

> The Go project does accept normal github pull requests: https://go.dev/doc/contribute#sending_a_change_github

Yes, but to contribute I need to sign a CLA, for which I need a Google account, for which I have to provide my phone number. I would not have found this bug if I didn't care about privacy. Requiring all contributors to get an account with Big Brother is just rude.

My pull request won't go through, but do feel free to use the code. I am providing it to the project under the project's license (although the patch is so small that it's probably not copyrightable).

ianlancetaylor commented on May 12 Contributor

@nervuri I completely understand not wanting to sign the CLA, but in that situation please don't send us code via GitHub pull requests or e-mail or in any other way. Our legal advice is very clear: we can only accept code changes from people who have signed the CLA. When you send us code without signing the CLA we have to be careful to not look at that code and not rely on it in any way in making our own changes. Thanks for understanding.

nervuri commented on May 12 • edited ▾ Author

I would be willing to sign the CLA if it didn't require using a Google account and providing Google my phone number. Golang could use Github's cla-bot, for instance. Or I'll just do it here: I hereby sign the CLA currently hosted at https://cla.developers.google.com/about/google-individual

Anyway, I closed the pull request - hope that makes it easier for you. I'm sure nobody looked at the code. :)

gopherbot commented on May 12

Change https://go.dev/cl/405994 mentions this issue: `crypto/tls: randomly generate ticket_age_add`

dmitshur added **NeedsFix** and removed **NeedsInvestigation** labels on May 17

dmitshur added this to the **Go1.19** milestone on May 17

cagedmantis commented on May 17 Contributor

This freeze exception has been approved.

dmitshur added the Security label on May 18

gopherbot closed this as completed in `fe4de36` on May 18

gopherbot commented on May 25

Change https://go.dev/cl/408574 mentions this issue: `[release-branch.go1.17] crypto/tls: randomly generate ticket_age_add`

gopherbot commented on May 25

Change https://go.dev/cl/408575 mentions this issue: `[release-branch.go1.18 crypto/tls: randomly generate ticket_age_add`

gopherbot pushed a commit that referenced this issue on May 27

`[release-branch.go1.18 crypto/tls: randomly generate ticket_age_add` … `c838098`

gopherbot pushed a commit that referenced this issue on May 27

`[release-branch.go1.17] crypto/tls: randomly generate ticket_age_add` … `c15a8e2`

tsaarni commented on Jun 10

Would it be possible to cast some more light for the reason for issuing CVE-2022-30629? As an outsider, this seems more like RFC 8446 non-compliance issue since the server does not use `obfusacted_ticket_age` (link).

tatianab mentioned this issue on Jul 25

x/vulndb: potential Go vuln in std: CVE-2022-30629 golang/vulndb#531

Closed

danbudris pushed a commit to danbudris/go that referenced this issue on Sep 9

`[release-branch.go1.17] crypto/tls: randomly generate ticket_age_add` … `3beb7c1`

danbudris pushed a commit to danbudris/go that referenced this issue on Sep 14

`[release-branch.go1.17] crypto/tls: randomly generate ticket_age_add` … `e25bfe0`

rcrozean pushed a commit to rcrozean/go that referenced this issue on Oct 5

`crypto/tls: randomly generate ticket_age_add` … `7ba3006`

rcrozean pushed a commit to rcrozean/go that referenced this issue on Oct 12

`crypto/tls: randomly generate ticket_age_add` … `82fb8a9`

rcrozean pushed a commit to rcrozean/go that referenced this issue on Oct 12

`crypto/tls: randomly generate ticket_age_add` … `e8849c6`

Assignees

No one assigned

Labels

NeedsFix Security

Projects

None yet

Milestone

Go1.19

Development

Successfully merging a pull request may close this issue.

crypto/tls: randomly generate ticket_age_add

11 participants