New issue

Jump to bottom

DTLS Fingerprints in SDP Offer/Answer are not verified #1708

Closed **gaukas** opened this issue on Mar 17, 2021 · 9 comments

gaukas commented on Mar 17, 2021 • edited

Your environment.

- Version: pion/webrtc v3.0.14
- Browser: N/A
- Other Information - reproducible with example/data-channels-create & example/data-channels

What did you do?

- Run both `data-channels-create` and `data-channels` from example.
- Once the SDP offer has been generated, decode it with base64.
- Randomly edit the DTLS fingerprint value in the SDP offer
- Copy & paste the base64-encoded SDP offer into the waiting `data-channels`
- Copy & paste the SDP answer generated by `data-channels` into `data-channels-create`

What did you expect?

The built-in fingerprints verification should throw an error and therefore prevent the data-channel from being established.

What happened?

The data channel was created as usual.

```
ICE Connection State has changed: checking
ICE Connection State has changed: connected
Data channel 'data'-'824635660400' open. Random messages will now be sent to any connected DataChannels every 5 seconds
Sending 'SBfBWYaFzaFZDiV'
Message from DataChannel 'data': 'EtaKTfGglNgpNNn'
```

Sean-Der commented on Mar 17, 2021 Member

Hey **@gaukas**

We do have a test for this `TestInvalidFingerprintCausesFailed` that is properly catching this. I will confirm this works and update as appropriate thanks for filing this!

👍 1

Sean-Der closed this as completed in `c901d6f` on Mar 17, 2021

Sean-Der commented on Mar 17, 2021 Member

Hey **@gaukas** what browser are you using to test?

I believe the remote peer isn't the one properly asserting.

thanks

gaukas commented on Mar 17, 2021 Author

I am not using any browser. The `offerer` is `data-channels-create` and the `answerer` is `data-channels`. Both are go binaries.

gaukas commented on Mar 17, 2021 Author

It may not be that simple because I tried to mess with both fingerprints in offer and answer. The data channel was still created successfully.

gaukas commented on Mar 17, 2021 Author

@Sean-Der but thank you for the fast response! I really appreciate it. Please let me know if there's anything else I could help with.

Sean-Der commented on Mar 17, 2021 • edited Member

Ah I see. So the issue is that we set PeerConnectionState to failed, but we don't actually tear down the connections.

I will fix that and tag a new release. This probably even warrants a CVE! If you are interested, good for resume and helps people update quicker.

gaukas commented on Mar 17, 2021 Author

Thank you **@Sean-Der**! I'm glad that this issue could be helpful to the project.
Just for your reference, attached is the log from both instances, in which `2 bytes` from the fingerprint in the offer (generated by `data-channels-create`) have been altered.

```
$ ./data-channels-create
eyJ0eXBlIjoib2ZmZXIiLCJzZHAiOiJ2PTBcclxubz0tIDgzNDg1NzQ2MDI2Njc1NjA4MDggMTYxNjAyMzA1NiBJTiBJUDQgMC4wLjAuMFxyXG5zPS1cclxudD0wIDBcclxuYT1maW5nZXJwcmludDpzaGEtMjU2IDgwOkJCOjI0OkU0OjE4OkI
eyJ0eXBlIjoiYW5zd2VyIiwic2RwIjoidj0wXHJcbm89LSA3MzM4NDEwODE4NDE3NTg5Njg2IDE2MTYwMjMwODAgSU4gSVA0IDAuMC4wLjBcclxucz0tXHJcbnQ9MCAwXHJcbmE9ZmluZ2VycHJpbnQ6c2hhLTI1NiAwOToyMzpFODpEQTpGRDp

ICE Connection State has changed: checking
ICE Connection State has changed: connected
Data channel 'data'-'824635376524' open. Random messages will now be sent to any connected DataChannels every 5 seconds
Sending 'AUBiqltUsGmfLdH'
Message from DataChannel 'data': 'oOPNoAVEGkOJytm'
Sending 'ONDrJkdvURrBMuc'
Message from DataChannel 'data': 'OVgMvURKIMJLKJY'
^C
```

```
$ ./data-channels
eyJ0eXBlIjoib2ZmZXIiLCJzZHAiOiJ2PTBcclxubz0tIDgzNDg1NzQ2MDI2Njc1NjA4MDggMTYxNjAyMzA1NiBJTiBJUDQgMC4wLjAuMFxyXG5zPS1cclxudD0wIDBcclxuYT1maW5nZXJwcmludDpzaGEtMjU2IDgwOkJCOjI0OkU0OjE4OkI

ICE Connection State has changed: checking
eyJ0eXBlIjoiYW5zd2VyIiwic2RwIjoidj0wXHJcbm89LSA3MzM4NDEwODE4NDE3NTg5Njg2IDE2MTYwMjMwODAgSU4gSVA0IDAuMC4wLjBcclxucz0tXHJcbnQ9MCAwXHJcbmE9ZmluZ2VycHJpbnQ6c2hhLTI1NiAwOToyMzpFODpEQTpGRDp
ICE Connection State has changed: connected
New DataChannel data 824637475034
Data channel 'data'-'824637475034' open. Random messages will now be sent to any connected DataChannels every 5 seconds
Sending 'oOPNoAVEGkOJytm'
Message from DataChannel 'data': 'AUBiqltUsGmfLdH'
Sending 'OVgMvURKIMJLKJY'
Message from DataChannel 'data': 'ONDrJkdvURrBMuc'
^C
```

Sean-Der added a commit that referenced this issue on Mar 17, 2021

`Close DTLS when fingerprint verification fails` … ✗ 465865e

Sean-Der mentioned this issue on Mar 17, 2021

Close DTLS when fingerprint verification fails #1709

Merged

Sean-Der commented on Mar 17, 2021 Member

Yea you were 100% right **@gaukas** before! The test we had wasn't very useful.

I fixed the issue and added a test mind trying #1709 ?

👍 1

Sean-Der added a commit that referenced this issue on Mar 17, 2021

`Close DTLS when fingerprint verification fails` … ✗ 9a1da17

Sean-Der added a commit that referenced this issue on Mar 17, 2021

`Close DTLS when fingerprint verification fails` … ✓ 545613d

gaukas commented on Mar 17, 2021 Author

Thanks for the fast response! Now I see the problem has been fixed.

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants