Open Bug 1334192 Opened 9 years ago Updated 3 years ago

common.tnode.com uses revoked certificate from StartCom

Categories

Product: Firefox ▾
Component: Security ▾
Platform: x86 macOS

Type: defect
Priority: P5 Severity: S3

Tracking

Status: UNCONFIRMED

People (Reporter: mmitar, Unassigned)

References (URL)

Details

Bottom ↓ Tags ▾ Timeline ▾

Mitar Reporter
Description • 9 years ago

User Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.10; rv:51.0) Gecko/20100101 Firefox/51.0
Build ID: 20170118123726

Steps to reproduce:

I tried to open https://common.tnode.com/

Actual results:

The following HTTPS error was shown: An error occurred during a connection to common.tnode.com. Peer's Certificate has been revoked. Error code: SEC_ERROR_REVOKED_CERTIFICATE

Expected results:

A 404 page should be displayed over HTTPS.

I checked and the certificate does not seem to be revoked:
https://www.ssllabs.com/ssltest/analyze.html?d=common.tnode.com

Mitar Reporter
Updated • 9 years ago

OS: Unspecified → Mac OS X
Hardware: Unspecified → x86

Tooru Fujisawa [:arai]
Comment 1 • 9 years ago

The certificate is issued by StartCom Certification Authority.

```
> Issuer        StartCom Certification Authority
```

and also "Valid from" is after October 21, 2016.

```
> Valid from    Fri, 28 Oct 2016 12:38:03 UTC
```

that's the reason why it's shown as revoked.

https://blog.mozilla.org/security/2016/10/24/distrusting-new-wosign-and-startcom-certificates/

```
> 1. Distrust certificates with a notBefore date after October 21, 2016 which chain
up to the following affected roots.
> ...
>   * This change will go into the Firefox 51 release train.
>   * The code will use the following Subject Distinguished Names to identify
>     the root certificates, so that the control will also apply to
>     cross-certificates of these roots.
> ...
>       * CN=StartCom Certification Authority, OU=Secure Digital Certificate
Signing, O=StartCom Ltd., C=IL
>       * CN=StartCom Certification Authority G2, OU=null, O=StartCom Ltd., C=IL
```

Loic
Comment 2 • 9 years ago

The webmaster needs to change the certificate, like one from Let's Encrypt.

URL: https://common.tnode.com/
Component: Untriaged → Desktop
Product: Firefox → Tech Evangelism
Summary: A site fails with SEC_ERROR_REVOKED_CERTIFICATE but certificate is not revoked → common.tnode.com uses revoked certificate from StartCom
Version: 51 Branch → Firefox 51

Mitar Reporter
Comment 3 • 9 years ago

Ah, error message could really be better. Because the error message looks like it is a certificate revoked by CA, not that Firefox revoked CA. This is really confusing and hard to debug. It would be also great if when I click "Learn more" I would be directed to this blog post linked above. Then I would understand what is happening.

Adam Stevenson [:adamopenweb]
Comment 4 • 9 years ago

I'm not sure there's a lot of value in doing outreach to the site here. Since the expected result is a 404. If someone wants to try, tnode.com links to: gwSPAM.2008@tnode.com.

Priority: -- → P5

Tooru Fujisawa [:arai]
Comment 5 • 9 years ago

Mitar, is https://common.tnode.com/ the actual URL that you want to open?
if not, what's the actual URL?

Tooru Fujisawa [:arai]
Comment 6 • 9 years ago

I googled "common.tnode.com" and I see some URLs under https://common.tnode.com/
not sure how they're used tho.

Mitar Reporter
Comment 7 • 9 years ago

OK, if this was unclear. I am a webmaster of the website at common.tnode.com. I understand now what is wrong, but I think that a better error message should be really helpful.

Karl Dubost 💡 **:karlcow**
Comment 8 • 9 years ago

Moving to Firefox Product as it is about UI and messaging.

Component: Desktop → General
Product: Tech Evangelism → Firefox
Version: Firefox 51 → unspecified

:Gijs (he/him)
Comment 9 • 8 years ago

Panos, do you know if there's anything we can improve here with some kind of reasonable cost/benefit? I expect that custom error codes just for this are a step too far, and the current infrastructure for these pages makes it difficult to do something else. We could hack something up by detecting this specific case in about:net/certerror, I guess... Alternatively, something to keep in mind for possible future deprecations etc.

Flags: needinfo?(past)

Panos Astithas (he/him) [:past] (please ni?)
Comment 10 • 8 years ago

I think keeler is in a better position to inform future deprecations. I believe the current message is fine from an end user's POV, but perhaps we could be more explicit in the web console (or in the error page advanced panel) for site authors.

Component: General → Security
Flags: needinfo?(past) → needinfo?(dkeeler)

Dana Keeler (she/her) [:keeler]
Comment 11 • 8 years ago

For a long time I've been wanting to develop a certificate linter in the browser that developers/website admins could use to determine what might be causing problems with their certificates. This item would be a great candidate for that. However, this project isn't on any roadmap yet, and it's not clear when it will be, if ever. That said, I imagine wosign/startcom isn't the last CA we'll have to impose restrictions on that are similar to this (see e.g. https://groups.google.com/a/chromium.org/forum/#!topic/blink-dev/eUAKwjihhBs%5B1-25%5D)

Flags: ~~needinfo?(dkeeler)~~

BMO Automation
Updated • 3 years ago

Severity: normal → S3

You need to log in before you can comment on or make changes to this bug.

Top ↑