pfSense - Todo #1438

Add override for CSR request->response subject mismatch

04/15/2011 12:44 AM - Yehuda Katz

Status:	Resolved	**Start date:**	04/15/2011
Priority:	Normal	**Due date:**	
Assignee:	Yehuda Katz	**% Done:**	80%
Category:	Certificates	**Estimated time:**	0.00 hour
Target version:	2.0		

Description

Just a bit of bug checking and the code that I mentioned on the mailing list will be ready (I am waiting on my CA to issue another cert).

Thoughts: another way (the proper way) to check whether a CSR and CERT match without checking the subjects.
Compare the outputs of:
openssl x509 -noout -modulus -in certificate.crt | openssl md5
openssl rsa -noout -modulus -in privateKey.key | openssl md5
openssl req -noout -modulus -in CSR.csr | openssl md5

History

#1 - 04/18/2011 02:24 PM - Yehuda Katz

- File system_certmanager.patch added

Here is the simple patch. A better one is on the way.

#2 - 04/18/2011 02:32 PM - Yehuda Katz

What I meant to say there is this patch fixes the problem.
I am working on a patch that will actually completely work around the problem by checking the modulus of the request and the response.

Also, I am not sure what happened to diff that the patch does not show up properly. Anyone know?

#3 - 04/18/2011 04:19 PM - Yehuda Katz

Better than a patch: I did a merge request on
https://rcs.pfsense.org/projects/pfsense/repos/yakatz-sandbox/commits/e2e934e0c976bae835b58de7c2595666ad59d2a0

#4 - 04/18/2011 10:13 PM - Chris Buechler

- Target version set to 2.0

#5 - 04/21/2011 05:27 PM - Yehuda Katz

New merge request sent

#6 - 04/27/2011 10:11 PM - Chris Buechler

tested this with a cert from namecheap, originally was seeing the issue described here, synced up to Yehuda's git clone and it then worked fine. Everything else looks to work as well, and the diff looks fine, needs another person to review.

#7 - 04/27/2011 10:13 PM - Yehuda Katz

My semester ends in about 2-3 weeks. At that point I will look around in the code for other places where this type of validation might be useful (maybe when creating regular certificates with public/private key).

#8 - 05/18/2011 11:49 PM - Yehuda Katz

I am not quite done yet, but I was looking at this ticket and there does not seem to be a way that I can update the percentage done field. I know it does not really matter, but I like to be complete if I can.

#9 - 05/22/2011 02:00 PM - Jim Pingle

Yehuda - That option is only available to users with certain levels of access here. If you want to just add a note on the ticket with the % done you want, someone with access can change that for you. It's at 80% now.

On an unrelated note, when this is complete, ticket #1318 can also be closed since this will fix the problem.

#10 - 05/22/2011 02:01 PM - Jim Pingle

Another note: Our repositories have moved from rcs.pfsense.org to github (https://github.com/bsdperimeter/pfsense), so you would need to make a new fork there and apply your patch, and then request a merge again if you want to go that route.

#11 - 05/22/2011 02:09 PM - Yehuda Katz

I already forked from GitHub and I am working from there.

I should have something to merge later today.

#12 - 05/23/2011 07:42 PM - Yehuda Katz

I was going through the files again and I found that there are no more places in the code that need this change.
This ticket can be marked as done.
My other SSL-related ticket (#1437) goes on...

#13 - 05/24/2011 01:28 AM - Chris Buechler

- Status changed from New to Resolved

thanks!

#14 - 05/24/2011 08:07 AM - Jim Pingle

I didn't see a commit bringing this into mainline, is the patch on the ticket up to date? I just want to make sure we get the right code in.

#15 - 05/24/2011 11:46 AM - Yehuda Katz

a828210b746c074c1e701a44f5f2ec3a69ba368a
2594f4010b85e5f4571ba76a69e36a16f441b4e3

#16 - 05/24/2011 11:49 AM - Jim Pingle

Ah, ok. I wasn't looking back far enough in the git log. Looks good, thanks!

Files

system_certmanager.patch	1.06 KB	04/18/2011	Yehuda Katz