pfSense - Bug #1437

More validation needed on CSR generation

04/14/2011 11:15 PM - Yehuda Katz

Status:	Resolved	**Start date:**	04/14/2011
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:	Certificates	**Estimated time:**	0.00 hour
Target version:	2.0		
Affected Version:	2.0	**Affected Architecture:**	

Description

It appears that if the countryName in the requested subject is not recognized by openssl, it throws these two errors (which show up at the top of the webconfigurator).
Warning: openssl_csr_new(): dn: add_entry_by_NID 14 -> _COUNTRY_NAME_ (failed) in /etc/inc/certs.inc on line 258
Warning: openssl_csr_export() expects parameter 1 to be resource, boolean given in /etc/inc/certs.inc on line 262
It appears to create a self signed cert, but I am not sure if that works.

Associated revisions

Revision 9d2d65f3 - 06/16/2011 11:04 PM - Evgeny Yurchenko

Bug #1437. Dropdown list for country codes (CA manager)

Revision 21cc2faa - 06/17/2011 12:41 AM - Evgeny Yurchenko

Bug #1437. Check for invalid characters in the fields for ca, cert and csr.

Revision 24cbe7a8 - 06/17/2011 12:57 AM - Evgeny Yurchenko

Bug #1437. Dropdown list for country codes for CSRs (Cert Manager)

History

#1 - 04/15/2011 12:32 AM - Chris Buechler

- Category set to Certificates

- Target version set to 2.0

- Affected Version set to 2.0

#2 - 05/18/2011 11:21 PM - Yehuda Katz

Three places call `openssl_csr_new(...)`.
None of those have any validation.
All three are in /etc/inc/certs.inc
I am not sure would be the proper way to return error messages from there is.
The code should be something like this:

```
  $res_csr = openssl_csr_new($dn, $res_key, $args);
+ if ($res_csr === false) {
+     while ( $msg = openssl_error_string() ) {
+         $errors[] = $msg;
+     }
+     return $errors;
+ }
  $res_crt = openssl_csr_sign($res_csr, null, $res_key, $lifetime, $args);
```

The trouble with this is the function return type could be an array.
It might be better to throw an exception since exceptions can contain data.

Similar changes might make sense around other openssl_ functions.
It might be worth creating a wrapper that will take any openssl_ function and catch its errors.

Maybe like this (note, I did not test this function:

```
/* takes function name without "openssl_" and regular function parameters */
function run_openssl_fun() {
    $args = func_get_args();
    $fn = array_shift($args);
    $result = call_user_func_array("openssl_$fn", $args);
    if ($result === false){
        while ( $msg = openssl_error_string() ) {
            $errors[] = $msg;
        }
        throw new Exception(implode("\r\n", $errors););
    }
    return $result;
}
```

Again, I did not test the function above.

#3 - 05/23/2011 03:51 PM - Yehuda Katz

Any comments on this potential solution?

#4 - 06/15/2011 10:08 AM - Ermal Luçi

Possible solution a listbox with values The solution for this probably is a listbox with values from
http://www.digicert.com/ssl-certificate-country-codes.htm

#5 - 06/15/2011 10:45 AM - Yehuda Katz

I don't think that is the proper solution to the problem. Hard-coding a country code list only works until the country list changes (which has happened several times in the last few years if I remember correctly.)
There could also be other problems with the csr generation besides the wrong country list.

The PHP OpenSSL extension does have error handling.
I tried out the code above, but the Exception that it throws never makes it out all the way to the rendered web page. If there a reason that exceptions don't get all the way through?

https://github.com/yakatz/pfsense/commit/c35a729da367b4b4f38e3564da1c507db1d86978

#6 - 06/15/2011 11:39 AM - Evgeny Yurchenko

I see two different questions here:
1. User input validation. Country name validation? whatever approach we use (dropdown list or something else) it will need to be changed if new country is added. Besides, it is impossible to validate other fields (validation for emptiness is already in place)

2. Error reporting. This should be done but I do not think Exceptions is right approach.

#7 - 06/15/2011 11:46 AM - Jim Pingle

Another thing we need to filter for is invalid characters in the fields for the certificate. A quick search turned up the following as invalid:

```
! @ # $ % ^ ( ) ~ ? > < & / \ , . " '
```

And a drop-down makes sense - if OpenSSL itself is rejecting the country code because it's invalid, then OpenSSL would need updated for a new country code as well. Why not limit the input to only what our version of OpenSSL believes is valid?

Exceptions, though useful, seem like overkill for this.

#8 - 06/15/2011 11:49 AM - Yehuda Katz

1. There are other possible errors in csr generation besides invalid input. I am also suggesting that this wrappr can be used around ANY openssl function, because I could not find any error handling at all for openssl functions currently in the code.

2. Exceptions might not be the right way to do it, but a wrapper function needs some way of returning errors.
It could return an array $re['errors'] and the caller would need to check for that.
I thought exceptions would be simpler since that is really exactly what they are designed for.

And, will someone remember every time openssl is updated to check whether this list needs to be updated?

#9 - 06/17/2011 01:02 AM - Evgeny Yurchenko

Adding countries now is just adding lines to the file /etc/ca_countries and could be easily done when needed.
Regarding drop-down lists and other input validations please see
https://github.com/bsdperimeter/pfsense/commit/9d2d65f3a3e0478b75a42086167c6520d31778c7
https://github.com/bsdperimeter/pfsense/commit/21cc2faa85e612169d98deca1f72fce9ff9260a5
https://github.com/bsdperimeter/pfsense/commit/24cbe7a895c78ce12cde907ab4994630391567e0
Now we need to think how to catch possible errors during openssl_xxx functions execution.

#10 - 06/23/2011 08:30 PM - Evgeny Yurchenko

Errors handling added:
https://github.com/bsdperimeter/pfsense/commit/95c8cf48f9bd72da5371aa01a03a070885411dbf
https://github.com/bsdperimeter/pfsense/commit/1b6d9fa59cdc3a284497abb0bfa415741c258d10
https://github.com/bsdperimeter/pfsense/commit/22b380aa6f4b7401b887945262a2e595d03dac26
Feedback?

#11 - 06/23/2011 09:19 PM - Yehuda Katz

I will test this on or right after July 4th. I will not have internet access between tomorrow and then (working at a Boy Scout camp for a week.)

#12 - 07/28/2011 05:06 PM - Ermal Luçi

- Status changed from New to Feedback

#13 - 08/13/2011 11:09 PM - Chris Buechler

Yehuda - is this fixed?

#14 - 09/06/2011 09:56 PM - Chris Buechler

- Target version deleted (2.0)

should be fixed, awaiting Yehuda's confirmation

#15 - 09/06/2011 10:06 PM - Yehuda Katz

I have so much going on, I thought I replied to this, but I guess I did not.

Everything that I did to cause an error actually resulted in an error message showing up, so I would say this is fixed.

#16 - 09/07/2011 07:08 PM - Chris Buechler

- Status changed from Feedback to Resolved

- Target version set to 2.0

thank you