pfSense - Bug #4605

OpenVPN user/pass fails if usernames and/or passwords contain special characters (reopen bugs 4177 and 4340)

04/13/2015 09:25 AM - Dave Crane

Status:	Resolved	**Start date:**	04/13/2015
Priority:	Normal	**Due date:**	
Assignee:	Renato Botelho	**% Done:**	100%
Category:	OpenVPN	**Estimated time:**	0.00 hour
Target version:	2.3		
Affected Version:	2.2.x	**Affected Architecture:**	

Description

The fix for bug 4177 (OpenVPN user/pass auth fails if passwords end on special characters.) doesn't completely resolve the issue.

Bug 4340 (after upgrade pfSense to 2.2, OpenVPN fails connect for login S&V (authorization by AD).) introduces the same incomplete fix from 4177 to the "username" field.

The lines in /usr/local/sbin/ovpn_auth_verify don't urlEncode the base64 encoding properly; base64 can produce three non-alphanum characters: =, + and /.

It should be:

```
# Base64 and urlEncode usernames and passwords
password=$(echo -n "${password}" | openssl enc -base64 | sed -e 's_=_%3D_g;s_+_%2B_g;s_/_%2F_g')
username=$(echo -n "${username}" | openssl enc -base64 | sed -e 's_=_%3D_g;s_+_%2B_g;s_/_%2F_g')
```

I believe the str_replace in /etc/inc/openvpn.auth-user.php isn't needed either.
According to: http://php.net/manual/en/reserved.variables.get.php, anything retrieved through $_GET is automatically urlDecoded.

I'd like to suggest a comment for clarity:

```
/* Any string retrieved through $_GET is automatically urlDecoded */
$username = base64_decode($_GET['username']);
$password = base64_decode($_GET['password']);
```

To duplicate the issue, please try the username and/or password: "00>00?0" to test.

Thanks

Associated revisions

Revision a3d88018 - 01/27/2016 09:34 AM - Edin Sarajlic

Fix #4605

After base64 encoding username/password, properly escape characters =,+,/
before submitting auth details

History

#1 - 06/09/2015 07:36 AM - Edin Sarajlic

I can confirm that the issue still exists in pfSense 2.2.2.

I can also confirm that Dave Crane's solution works.

I will shortly be making a Pull Request on GitHub (credit goes to Dave Crane for the solution).

Testing:

Username (provided in OP): **00>00?0**
Password (my password that was causing authentication to fail): **RCAQ_!m}Q]doxtU6H>cA^T?B,**

What the username and password should be when base64 encoded:

```
$ echo -n '00>00?0' | base64
MDA+MDA/MA==
```

```
$ echo -n 'RCAQ_!m}Q]doxtU6H>cA^T?B,' | base64
UkNBUV8hbX1RXWRveHRVNkg+Y0FeVD9CLA==
```

As noted by Dave Crane in ticket #4177, base64 encoding can produce three non-alphanum characters: =, + and /.

These 3 characters are reserved, see "2.2. Reserved Characters" in http://www.faqs.org/rfcs/rfc3986.html . Currently after base64 encoding, only '=' is escaped/urlencoded (see: https://github.com/pfsense/pfsense/blob/472669b62634acc8d2e68aa3f899b91fafd56cd4/usr/local/sbin/ovpn_auth_verify#L7).

To help test, I added some logging code to /etc/inc/openvpn.auth-user.php:

```
syslog(LOG_ERR, "username is (base64 encoded):".  $_GET['username']);
syslog(LOG_ERR, "password is (base64 encoded):".  $_GET['password']);
```

After I'd attempted to authenticate, the log contained (notice that the '+' is missing):

```
openvpn: username is (base64 encoded):MDA MDA/MA==
openvpn: password is (base64 encoded):UkNBUV8hbX1RXWRveHRVNkg Y0FeVD9CLA==
```

After applying the patch, I attempted to authenticate again. This time the log contained:

```
openvpn: username is (base64 encoded):MDA+MDA/MA==
openvpn: password is (base64 encoded):UkNBUV8hbX1RXWRveHRVNkg+Y0FeVD9CLA==
```

On a final note, I'm now able to authenticate successfully with my (previously failing) password.

I've tested a few other passwords, and authentication is working correctly.

#2 - 06/09/2015 07:41 AM - Edin Sarajlic

Github Pull Request: https://github.com/pfsense/pfsense/pull/1711

#3 - 06/09/2015 08:03 AM - Edin Sarajlic

Sorry, my original pull request (#1711) referenced the wrong bug number.

Please see this Github Pull Request: https://github.com/pfsense/pfsense/pull/1712

#4 - 06/09/2015 01:00 PM - Kill Bill

Edin Sarajlic wrote:

> Testing:
> Username (provided in OP): **00>00?0**

I think you should read the fine POSIX. Seriously, the only thing that needs to be fixed here is preventing people ever being allowed to input similar ridiculous **beep**

#5 - 01/27/2016 09:24 AM - Renato Botelho

- Target version set to 2.3

#6 - 01/27/2016 09:24 AM - Renato Botelho

- Assignee set to Renato Botelho

#7 - 01/27/2016 09:30 AM - Edin Sarajlic

- Status changed from New to Feedback

- % Done changed from 0 to 100

Applied in changeset a3d88018522c0cb30501cb5e4a18ea881230bbc9.

#8 - 02/04/2016 03:06 AM - Jim Thompson

bump (a month in feedback)

#9 - 02/04/2016 03:56 AM - Renato Botelho

- Status changed from Feedback to Resolved

Works

#10 - 03/31/2016 08:12 PM - Chris Buechler

- Affected Version changed from 2.2.1 to 2.2.x