pfSense - Bug #7230

wizard.php - update_config_field() uses eval to set a value in a way that allows variable protections to be bypassed

02/07/2017 01:29 PM - Jim Pingle

Status:	Resolved	**Start date:**	02/07/2017
Priority:	Urgent	**Due date:**	
Assignee:	Jim Pingle	**% Done:**	100%
Category:	Web Interface	**Estimated time:**	0.00 hour
Target version:	2.3.3		
Plus Target Version:		**Affected Version:**	All
Release Notes:	Default	**Affected Architecture:**	All

Description

update_config_field() in wizard.php needs to use eval to construct a variable name that is several array levels deep. The problem lies in the way the value is set for this variable, it can be bypassed in various ways, including using passthru to escape addslashes.

It's easiest to test by using the OpenVPN wizard, get to the step with the interface selection and use firebug to alter the interface value to be"

```
wan";echo exec("id");"
```

Associated revisions

Revision 5baea4da - 02/07/2017 01:30 PM - Jim Pingle

Rather than setting the value directly, minimize exposure to eval() in update_config_field() from wizard.php by constructing a variable reference, then set the value using the reference rather than passing user input through eval(). Fixes #7230

Revision 2c5c799a - 02/07/2017 01:31 PM - Jim Pingle

Rather than setting the value directly, minimize exposure to eval() in update_config_field() from wizard.php by constructing a variable reference, then set the value using the reference rather than passing user input through eval(). Fixes #7230

Revision d3da9c7d - 02/07/2017 01:31 PM - Jim Pingle

Rather than setting the value directly, minimize exposure to eval() in update_config_field() from wizard.php by constructing a variable reference, then set the value using the reference rather than passing user input through eval(). Fixes #7230

History

#1 - 02/07/2017 01:40 PM - Jim Pingle

- Status changed from Confirmed to Feedback

- % Done changed from 0 to 100

Applied in changeset 5baea4da88fd6c093582d9c3e9b67cce5d6a1013.

#2 - 02/07/2017 08:34 PM - Jim Pingle

- Status changed from Feedback to Resolved

Fixed

#3 - 02/10/2017 10:20 AM - Jim Pingle

- Target version changed from 2.4.0 to 2.3.3

#4 - 03/21/2017 08:35 AM - Jim Pingle

- Private changed from Yes to No

#5 - 03/21/2017 08:36 AM - Jim Pingle

- Private changed from No to Yes

#6 - 03/21/2017 09:07 AM - Jim Pingle

- Private changed from Yes to No