pfSense - Bug #9061

PowerD command parameter validation and escaping

10/23/2018 11:46 AM - Jim Pingle

Status:	Resolved	**Start date:**	10/23/2018
Priority:	Urgent	**Due date:**	
Assignee:	Jim Pingle	**% Done:**	100%
Category:	Hardware / Drivers	**Estimated time:**	0.00 hour
Target version:	2.4.4-p1		
Plus Target Version:		**Affected Version:**	All
Release Notes:	Default	**Affected Architecture:**	All

Description

The powerd parameters powerd_ac_mode, powerd_battery_mode, and powerd_normal_mode are not validated against the list of expected mode strings in /usr/local/www/system_advanced_misc.php. They are also not escaped before use when invoking the powerd command inside activate_powerd() from /etc/inc/system.inc.

This can lead to an authenticated command injection for users with access to that page.

Associated revisions

Revision 3be69929 - 10/23/2018 12:13 PM - Jim Pingle

Validate and protect powerd option values. Fixes #9061

Revision c95a79d3 - 10/23/2018 12:14 PM - Jim Pingle

Validate and protect powerd option values. Fixes #9061

(cherry picked from commit 3be699295e5cb7be24cc5361700be1a8b759e26c)

History

#1 - 10/23/2018 12:20 PM - Jim Pingle

- Status changed from Assigned to Feedback

- % Done changed from 0 to 100

Applied in changeset 3be699295e5cb7be24cc5361700be1a8b759e26c.

#2 - 11/02/2018 04:23 PM - Anonymous

Could recreate the behavior on 2.4.4. On 2.4.5.a.20181102.0213, could not reproduce the behavior, received

```
The following input errors were detected:

    Invalid Battery Power mode.
```

after modifying the value of Battery Power mode and clicking Save.

#3 - 11/02/2018 04:23 PM - Anonymous

- Status changed from Feedback to Resolved

#4 - 12/03/2018 09:57 AM - Jim Pingle

- Private changed from Yes to No