pfSense - Bug #8302

traffic_graphs.widget.php potential XSS via settings

01/29/2018 11:23 AM - Jim Pingle

Status:	Resolved	**Start date:**	01/29/2018
Priority:	Normal	**Due date:**	
Assignee:	Jim Pingle	**% Done:**	100%
Category:	Dashboard	**Estimated time:**	0.00 hour
Target version:	2.4.3		
Affected Version:	2.4.x	**Affected Architecture:**	All

Description

traffic_graphs.widget.php does not perform input validation on its settings, which can lead to a potential XSS due to the way the settings are used in JavaScript.

The widget needs input validation and to encode the setting output before use.

Associated revisions

Revision e7b5b82b - 01/29/2018 11:26 AM - Jim Pingle

Add input validation to traffic_graphs_widget.php and fix JS encoding. Fixes #8302

Revision f51de9fd - 01/29/2018 11:27 AM - Jim Pingle

Add input validation to traffic_graphs_widget.php and fix JS encoding. Fixes #8302

(cherry picked from commit e7b5b82b121c76c4c6bf57229bfef0ea3bc33d5b)

History

#1 - 01/29/2018 11:40 AM - Jim Pingle

- Status changed from Confirmed to Feedback

- % Done changed from 0 to 100

Applied in changeset e7b5b82b121c76c4c6bf57229bfef0ea3bc33d5b.

#2 - 03/08/2018 01:45 PM - James Dekker

On 2.4.2 CE, added traffic graph widget to dash, set refresh interval to 1s, saved, backed up config and edited the config.xml to replace
<refreshinterval>1</refreshinterval>
with
<refreshinterval>"/><script>alert(1)</script></refreshinterval>

after the reboot, logged in and got an alert popup on the dashboard.

Upgraded to 2.4.3.a.20180308.0936, logged in, no alert popup on the dashboard, backed up config,
<refreshinterval>"/><script>alert(1)</script></refreshinterval>
still present in the config.

Cannot paste text with letters into the refresh interval field in Widget settings, results in "e1" showing up in the field. Also cannot type letters into the field.

Appears fixed.

#3 - 03/08/2018 02:26 PM - Jim Pingle

- Status changed from Feedback to Resolved

#4 - 03/29/2018 12:46 PM - Jim Pingle

- Private changed from Yes to No