pfSense - Bug #6737

diag_dns.php: DNS results printed without encoding, leading to an XSS

08/22/2016 11:30 AM - Jim Pingle

Status:	Resolved	**Start date:**	08/22/2016
Priority:	High	**Due date:**	
Assignee:	Jim Pingle	**% Done:**	100%
Category:	Web Interface	**Estimated time:**	0.00 hour
Target version:	2.3.2-p1		
Plus Target Version:		**Affected Version:**	All
Release Notes:	Default	**Affected Architecture:**	All

Description

There is a potential XSS in diag_dns.php from a lack of encoding on the DNS replies.

If a query is entered for xss.uparo.com, a script alert is shown.

Associated revisions

Revision d2466ce6 - 08/22/2016 11:29 AM - Jim Pingle

Add output encoding to diag_dns.php for results returned from DNS. Fixes #6737

Revision 9cbc340f - 08/22/2016 11:30 AM - Jim Pingle

Add output encoding to diag_dns.php for results returned from DNS. Fixes #6737

Revision a92de66e - 08/22/2016 11:30 AM - Jim Pingle

Add output encoding to diag_dns.php for results returned from DNS. Fixes #6737

History

#1 - 08/22/2016 11:40 AM - Jim Pingle

- Status changed from Assigned to Feedback

- % Done changed from 0 to 100

Applied in changeset d2466ce6f5f45300ebeccea93ef4b7c35f8e1f02.

#2 - 09/23/2016 10:23 AM - Jim Pingle

- Status changed from Feedback to Resolved

#3 - 02/09/2017 03:52 PM - Jim Pingle

- Private changed from Yes to No