

## pfSense - Bug #7227

### pkg.php - "pkg\_filter" is not encoded before output

02/07/2017 10:45 AM - Jim Pingle

<b>Status:</b>	Resolved	<b>Start date:</b>	02/07/2017
<b>Priority:</b>	Very High	<b>Due date:</b>	
<b>Assignee:</b>	Jim Pingle	<b>% Done:</b>	100%
<b>Category:</b>	Package System	<b>Estimated time:</b>	0.00 hour
<b>Target version:</b>	2.3.3	<b>Affected Architecture:</b>	All
<b>Affected Version:</b>	All		

#### Description

On pkg.php "pkg\_filter" is not encoded before output - It requires a package use pkg.php and that it has include\_filtering\_inputbox along with a field type that enables sorting. This can be used as a potential XSS vector.

Currently the only package using this combination is FreeRADIUS ( freeradius.xml and freeradiusauthorizedmacs.xml ) but it's a general issue in pkg.php

Affects 2.4 and 2.3.x

#### Associated revisions

##### Revision 6ac61204 - 02/07/2017 10:45 AM - Jim Pingle

Encode the contents of pkg\_filter before output. Fixes #7227

##### Revision 7100f041 - 02/07/2017 10:48 AM - Jim Pingle

Encode the contents of pkg\_filter before output. Fixes #7227

##### Revision ed7bfaa4 - 02/07/2017 10:48 AM - Jim Pingle

Encode the contents of pkg\_filter before output. Fixes #7227

#### History

##### #1 - 02/07/2017 10:50 AM - Jim Pingle

- Status changed from Confirmed to Feedback

- % Done changed from 0 to 100

Applied in changeset [6ac61204bc9e4cff54c818ecc71d20d2626a02e1](#).

##### #2 - 02/07/2017 08:31 PM - Jim Pingle

- Status changed from Feedback to Resolved

Fixed

##### #3 - 02/10/2017 10:21 AM - Jim Pingle

- Target version changed from 2.4.0 to 2.3.3

##### #4 - 03/21/2017 08:39 AM - Jim Pingle

- Private changed from Yes to No