pfSense - Bug #9390

diag_backup.php: Backup output generation failure with CSRF script tag inserted into XML

03/10/2019 04:59 PM - Sam Likins

Status:	Resolved	**Start date:**	03/10/2019
Priority:	Normal	**Due date:**	
Assignee:	Jim Pingle	**% Done:**	100%
Category:	Backup/restore	**Estimated time:**	0.00 hour
Target version:	2.4.4-p3		
Affected Version:	2.4.4_2	**Affected Architecture:**	All

Description

Since the last update (ie: **2.4.4_2**), backups fail to restore; previously generated backups will restore, but new backups will fail restoration with the following message:

```
The following input errors were detected:

 - The configuration could not be restored.
```

When creating a backup XML file, regardless of the options (Backup area, Skip packages, Skip RRD data, Encryption) the generated file has an erroneous line at the end, outside the pfSense closing tag. you erroneous line is the following:

```
<script type="text/javascript">CsrfMagic.end();</script>
```

This CSRF line is added by the output buffer function **csrf_ob_handler** in the file **/usr/local/www/csrf/csrf-magic.php**. The generation of the backup file occurs in file **/usr/local/www/diag_backup.php** on line 228. Due to the CSRF output buffer flag **js-rewrite** being enabled when the backup is output, the erroneous line is added.

```
$GLOBALS['csrf']['rewrite-js']
```

This global value needs to be set to false prior to outputting the backup.

BUG FIX to be submitted shortly.

Associated revisions

Revision 4015b03d - 03/10/2019 06:43 PM - Jim Pingle

Fix output buffering when downloading config backups. Fixes #9390

Revision 428f6f02 - 03/10/2019 06:44 PM - Jim Pingle

Fix output buffering when downloading config backups. Fixes #9390

(cherry picked from commit 4015b03d4b184e546cb3590430fee6f9953ce23e)

History

#1 - 03/10/2019 05:35 PM - Tim Harman

I can't reproduce this.

[2.4.4-RELEASE-p2 (amd64)
built on Wed Dec 12 07:40:18 EST 2018
FreeBSD 11.2-RELEASE-p6]

A full backup, using the WebGUI (with RRD data included, or excluded) finishes as expected with </pfsense> and nothing further.
Is there something else that's required to trigger this?

#2 - 03/10/2019 05:39 PM - Sam Likins

PR #4055 Created

#3 - 03/10/2019 05:47 PM - Jim Pingle

- File backup-buffer-fix.diff added

- Assignee set to Jim Pingle

That PR is the wrong fix.

I haven't been able to reproduce this here, but it appears to be due to output buffering.

See https://forum.netgate.com/post/822829

The attached patch fixes it properly, but since I can't reproduce it I've been waiting on additional confirmation that it works. It worked for one person on the thread linked above.

#4 - 03/10/2019 05:52 PM - Sam Likins

That is a bad solution, performing unnecessary complexity, when turning off the flag prior to outputting the payload focuses the solution to the issue.

#5 - 03/10/2019 05:54 PM - Sam Likins

Look at PR 4055: https://github.com/pfsense/pfsense/pull/4055

#6 - 03/10/2019 05:59 PM - Jim Pingle

You're entitled to your opinion but I disagree. Output buffering can cause other issues with downloading other than the case you are seeing, and this fixes all potential sources of problems and not the single case covered by the other fix. See #9239

#7 - 03/10/2019 06:50 PM - Jim Pingle

- Status changed from New to Feedback

- % Done changed from 0 to 100

Applied in changeset 4015b03d4b184e546cb3590430fee6f9953ce23e.

#8 - 03/11/2019 06:53 PM - Jim Pingle

Two reports of success with the committed patch, for different issues as well:

https://forum.netgate.com/post/825828
https://forum.netgate.com/topic/141378/issues-with-update-to-2-4-2_2

#9 - 03/12/2019 10:55 AM - Jim Pingle

- Target version changed from 48 to 2.5.0

#10 - 05/11/2019 04:48 PM - Jim Pingle

- Target version changed from 2.5.0 to 2.4.4-p3

#11 - 05/16/2019 11:35 AM - Jim Pingle

- Status changed from Feedback to Resolved

Unable to reproduce on -p3. Looks good all around.

No CSRF string in a previously affected system, and also a complete configuration download from a system that previously cut off early due to output buffering.

Files

backup-buffer-fix.diff	471 Bytes	03/10/2019	Jim Pingle