pfSense - Bug #3840

Disable (or give the option to disable) the OS addition to the SSH daemon banner

08/29/2014 02:33 PM - Jim Pingle

Status:	Resolved	**Start date:**	08/29/2014
Priority:	Normal	**Due date:**	
Assignee:	Renato Botelho	**% Done:**	100%
Category:	Operating System	**Estimated time:**	0.00 hour
Target version:	2.2		
Affected Version:	All	**Affected Architecture:**	All

Description

By default ssh on FreeBSD adds a VersionAddendum of the FreeBSD version in use. It would be best to hide that to avoid broadcasting the OS version to anyone who can connect to the SSH port.

We can add a line with the VersionAddendum directive only (no parameters) to use an empty version

```
: nc localhost 22
SSH-2.0-OpenSSH_5.4p1_hpn13v11 FreeBSD-20100308
^C
: echo VersionAddendum >> /etc/sshd_config
: killall -HUP sshd
: nc localhost 22
SSH-2.0-OpenSSH_5.4p1_hpn13v11
^C
```

Associated revisions

Revision 729ca302 - 08/29/2014 03:13 PM - Renato Botelho

Hide FreeBSD version from sshd banner. It fixes #3840

Revision 2b56c7da - 08/29/2014 03:26 PM - Renato Botelho

Hide FreeBSD version from sshd banner. It fixes #3840

History

#1 - 08/29/2014 03:20 PM - Renato Botelho

- Status changed from New to Feedback

- % Done changed from 0 to 100

Applied in changeset 729ca302e389f63e0bc3432f57424123312f3e63.

#2 - 08/29/2014 03:30 PM - Renato Botelho

Applied in changeset 2b56c7da667daaba0e34720138e105de7f7bf7e5.

#3 - 09/01/2014 11:42 AM - Jim Thompson

- Assignee set to Renato Botelho

JimP, you realize this does nothing, right?

#4 - 09/03/2014 12:46 PM - Jim Pingle

- Status changed from Feedback to Resolved

Tested on a current snapshot, FreeBSD version is gone now. Looks good.

Jim Thompson wrote:

> JimP, you realize this does nothing, right?

Functionally, yes, it only hides the FreeBSD version string and doesn't fix anything.

But with the OS version present in the banner scanners assume it's FreeBSD 8.3 and whinge about the version being unsupported. Which isn't true in our case since it's not FreeBSD 8.3, but pfSense 2.1.x, where we maintain our own security patches. It's safer to err on the side of caution and not provide anyone who can connect to the SSH port with more information than they need. None of the other commonly-exposed daemons advertise the exact FreeBSD version in the same way.

If nothing else, it will at least stop automated scanners from incorrectly flagging pfSense as "outdated" which has caused users to fail audits. That part will be a non-issue once 2.2 is out but IMO it's still best to not hand out more info than required for clients to safely connect.

#5 - 09/03/2014 01:12 PM - Renato Botelho

What about add pfSense version instead of FreeBSD's?

#6 - 09/03/2014 01:13 PM - Jim Pingle

Personally I'd prefer to omit any extra information rather than announcing that willingly.