pfSense - Bug #10155

sshguard is not compatible with RFC 5424 log format

01/03/2020 11:14 AM - Jim Pingle

Status:	Resolved	**Start date:**	01/03/2020
Priority:	Normal	**Due date:**	
Assignee:	Jim Pingle	**% Done:**	0%
Category:	Logging	**Estimated time:**	0.00 hour
Target version:	2.5.0		
Plus Target Version:		**Affected Version:**	2.5.0
Release Notes:	Default	**Affected Architecture:**	All

Description

pfSense 2.5.0 has an option to change the syslog style from the default RFC 3154 format to the new RFC 5424 format. However, sshguard does not appear to parse the messages properly when fed RFC 5424 format log data.

I tested with ssh messages so it shouldn't be anything specific to pfSense at play here.

History

#1 - 01/03/2020 11:56 AM - Jim Pingle

- Assignee deleted (Jim Pingle)

Brief review didn't turn up any options that might help, and I didn't see any similar format messages in the sshguard tests.txt list. I opened an issue upstream with sshguard: https://bitbucket.org/sshguard/sshguard/issues/124/sshguard-does-not-parse-rfc-5424-format

If it isn't addressed before we need to ship 2.5.0, then we should at least add a warning to the syslog format selection option in the GUI alerting the user to the potential danger of using the other format.

#2 - 05/15/2020 07:58 AM - Jim Pingle

sshguard has added support for this log format in their repo, but it has not yet been released. Something to watch out for: https://bitbucket.org/sshguard/sshguard/commits/c18687f

#3 - 09/21/2020 12:15 PM - Renato Botelho

sshguard 2.4.1 is now imported into pfSense 2.5.0

#4 - 09/21/2020 12:16 PM - Renato Botelho

- Status changed from New to Feedback

- Assignee set to Jim Pingle

#5 - 09/22/2020 08:26 AM - Jim Pingle

- Status changed from Feedback to Resolved

This looks good now, thanks!

```
<38>1 2020-09-22T09:23:54.244277-04:00 pfsense.home.arpa sshd 93676 - - Invalid user blah from 198.51.100.148
port 16703
<38>1 2020-09-22T09:23:54.259618-04:00 pfsense.home.arpa sshd 93676 - - Postponed keyboard-interactive for inv
alid user blah from 198.51.100.148 port 16703 ssh2 [preauth]
<37>1 2020-09-22T09:23:54.281547-04:00 pfsense.home.arpa sshguard 7044 - - Attack from "198.51.100.148" on ser
vice SSH with danger 10.
```

```
<35>1 2020-09-22T09:23:55.452488-04:00 pfsense.home.arpa sshd 93676 - - error: PAM: Authentication error for i
llegal user blah from 198.51.100.148
<38>1 2020-09-22T09:23:55.453918-04:00 pfsense.home.arpa sshd 93676 - - Failed keyboard-interactive/pam for in
valid user blah from 198.51.100.148 port 16703 ssh2
<37>1 2020-09-22T09:23:55.455279-04:00 pfsense.home.arpa sshguard 7044 - - Attack from "198.51.100.148" on ser
vice SSH with danger 10.
<38>1 2020-09-22T09:23:55.461549-04:00 pfsense.home.arpa sshd 93676 - - Postponed keyboard-interactive for inv
alid user blah from 198.51.100.148 port 16703 ssh2 [preauth]
<35>1 2020-09-22T09:23:56.717308-04:00 pfsense.home.arpa sshd 93676 - - error: PAM: Authentication error for i
llegal user blah from 198.51.100.148
<38>1 2020-09-22T09:23:56.718296-04:00 pfsense.home.arpa sshd 93676 - - Failed keyboard-interactive/pam for in
valid user blah from 198.51.100.148 port 16703 ssh2
<37>1 2020-09-22T09:23:56.718801-04:00 pfsense.home.arpa sshguard 7044 - - Attack from "198.51.100.148" on ser
vice SSH with danger 10.
<36>1 2020-09-22T09:23:56.718916-04:00 pfsense.home.arpa sshguard 7044 - - Blocking "198.51.100.148/32" for 12
0 secs (3 attacks in 2 secs, after 1 abuses over 2 secs.)
```