pfSense Packages - Bug #8454

Arpwatch package break email notifications from other sources

04/12/2018 07:18 AM - Yehuda Katz

Status:	New	**Start date:**	04/12/2018
Priority:	Very Low	**Due date:**	
Assignee:		**% Done:**	0%
Category:	arpwatch	**Estimated time:**	0.00 hour
Target version:			
Affected Version:	2.4.3	**Affected Architecture:**	All

Description

Arpwatch replaces /usr/sbin/sendmail with a symlink to a PHP script that specifically mentioned Arpwatch in the message subject: https://github.com/pfsense/FreeBSD-ports/blob/015971be238550a1f9aa060fe5ed93849c01572e/net-mgmt/pfSense-pkg-arpwatch/files/usr/local/pkg/arpwatch.inc#L217

This causes notifications from ACME (run by CRON) to come with subjects like this:

> wall.example.com - Arpwatch Notification : Cron <root@wall> /usr/local/pkg/acme/acme_command.sh "renewall"

History

#1 - 04/12/2018 07:34 AM - Jim Pingle

- Category set to arpwatch

- Priority changed from Normal to Very Low

I wouldn't say those are broken. Those cron notifications didn't work at all without the symlink setup by arpwatch. Firewalls without that package would never see those e-mails since the base system doesn't have a mail program at that location.

So it enables those other notifications, but they are mislabeled.

Notifications using the pfSense SMTP notifications settings, sent by pfSense code and not enabled by that symlink, still work properly.

#2 - 04/13/2018 09:48 AM - Yehuda Katz

Makes sense since all that sendmail script does is call the internal mail handling.

I see three options:
1. Change the sendmail supplied by arpwatch to be more generic (and possibly add the same to the cron package)
2. Add a separate pfSense-pkg-sendmail
3. Add a generic sendmail script to the core.

I would be happy to supply a patch for any of those. Do you have a preference?

#3 - 07/17/2018 08:12 AM - Matt Castelein

I don't like how this works either. The arpwatch package shouldn't be stepping on other notifications. Additionally, if ACME is supposed to be able to send notifications but cannot, that's a defect as well.

#4 - 07/17/2018 08:23 AM - Jim Pingle

There is no "stepping on other notifications".

It was not seen before because there was no "sendmail" on the box for cron to use. It doesn't need it, but if it's there it will use it. ACME doesn't need cron to send notifications. The mail message noted above is from cron, not ACME. In this case it only sent a message because the cron script generated some output that it probably didn't need to do, which resulted in the cron message.

arpwatch notifications can't work any other way than by using sendmail as far as I'm aware. If there is some other way to handle them, I'd love to see it.

#5 - 07/17/2018 08:35 AM - Matt Castelein

It's stepping on it in that it's putting "arpwatch" on an email that has nothing to do with arpwatch. ~~I'd actually prefer to be able to stop cron sending mail.~~ I guess I can do this by installing the Cron package. Then I can redirect the output to null, and the changes will survive a reboot.

#6 - 08/07/2018 11:30 AM - Joshua Diamant

I am also having this issue now that I installed arpwatch. I am starting to get emails from cron and other packages since arpwatch created '/bin/sbin/sendmail'

Can we change arpwatch so it installs a local sendmail script in a non-standard directory?

If not, can we change arpwatch to use mailreport instead of /bin/sbin/sendmail?

#7 - 08/07/2018 11:39 AM - Jim Pingle

Arpwatch cannot be configured to use an alternate sendmail or mail delivery mechanism.

#8 - 08/07/2018 11:53 AM - Joshua Diamant

Jim Pingle wrote:

> Arpwatch cannot be configured to use an alternate sendmail or mail delivery mechanism.

Cant we edit line 23 of the arpwatch.inc file (https://github.com/pfsense/FreeBSD-ports/blob/015971be238550a1f9aa060fe5ed93849c01572e/net-mgmt/pfSense-pkg-arpwatch/files/usr/local/pkg/arpwatch.inc#L23) to point to something other than '/usr/sbin/sendmail'

Can we point it to '/usr/sbin/sendmail-arpwatch' which symlinks to /usr/local/arpwatch/sendmail_proxy.php

#9 - 08/07/2018 12:06 PM - Jim Pingle

No, because that only manages the name of the link created by the script, it does not control what arpwatch uses.

#10 - 08/07/2018 12:18 PM - Yehuda Katz

The Debian port of Arpwatch allows you to specify a different sendmail program, but I don't think that is in the version available here.
Also on Linux, there are several different ways to get the name of the calling process and use that in the script, but I am not sure how to do that in BSD.
If anyone knows, I would be happy to write a sendmail script that can use that information to send better emails.

#11 - 09/01/2019 02:50 AM - Ter Ted

This issue forced me to uninstall arpwatch, as I can't just handle receive tons of emails from other daemons (like ClamAV) send as Arpwatch. I haven't got any issues before I install Arpwatch. It could be easily fixed by removing/redirecting notifications in cron, but PFSesne doesn't allow to edit cron (it doesn't survive reboot). It was very annoying, I don't understand why it can't be fixed.

#12 - 11/07/2019 08:36 AM - Christian Rhomberg

Hi, is there a chance this problem will be fixed?