pfSense - Bug #3585

CVE-2014-0160 - OpenSSL Heartbleed Bug

04/08/2014 04:32 AM - Doktor Notor

Status:	Resolved	**Start date:**	04/08/2014
Priority:	Urgent	**Due date:**	
Assignee:		**% Done:**	0%
Category:	Operating System	**Estimated time:**	0.00 hour
Target version:	2.1.2		
Affected Version:	All	**Affected Architecture:**	All

Description

Marking as urgent, see http://heartbleed.com/

History

#1 - 04/08/2014 09:07 AM - Steve Thomas

+1111111

#2 - 04/09/2014 05:19 AM - Nils Bernhardt

PFsense 2.1 uses openssl 0.9.8y, which is NOT VULNERABLE.

#3 - 04/09/2014 05:25 AM - Nils Bernhardt

OK, my fault: find / -type f -name 'openssl' -exec \{\} version \;

> OpenSSL 1.0.1e 11 Feb 2013
> OpenSSL 0.9.8y 5 Feb 2013

So we ARE VULNERABLE...

#4 - 04/09/2014 05:26 AM - Oliver Schonrock

that's true only for the base system.

but several packages including lighttpd for the webfrontend use /usr/local/bin/openssl (ie openssl from ports /usr/ports/security/openssl) which, pfsense 2.1.1 is:

1. /usr/local/bin/openssl version
   OpenSSL 1.0.1f 6 Jan 2014

This is vulnerable, and that make the web frontend vulnerable.

Also if you read the FreeBSD secruity advisories from today, there is one that is applicable to the base system openssl (not heartbleed, but different);

http://www.freebsd.org/security/advisories/FreeBSD-SA-14:06.openssl.asc
CVE-2014-0076

So that needs patching as well.

#5 - 04/09/2014 05:27 AM - Frederic MEYER

Unfortunately.
Check the https://redmine.pfsense.org/issues/3588 to watch the progress.

#6 - 04/10/2014 10:20 AM - Jim Pingle

FYI- 2.1.2 images are being tested now. So far, so good.

As a reminder, this bug is for Heartbleed in the base system. For issues with packages, see #3588

#7 - 04/10/2014 02:38 PM - Chris Buechler

- Status changed from New to Resolved

- Target version set to 2.1.2

fixed