Packages - Packaging Request #2138

[systemd] affected by CVE-2018-16865, CVE-2018-16864, CVE-2018-6954, CVE-2018-16866. High risk!

2019-01-14 12:06 AM - anon7mous

Status:	fixed	**% Done:**	0%
Priority:	wish		
Assignee:			
Category:			

Description

Update to 240.0-3!
Reported yesterday as outdated but no update.

History

#1 - 2019-01-14 02:04 AM - freemor

Thanks for bringing this up. But:

These are all LOCAL exploits which means that unless someone is already in your machine they are not that big a concern.
Also please understand that the Parabola crew is Small and voluntary labour done in spare time. (No full time paid staff). So It'll take a bit longer for someone to assess the situation, apply the updates while maintaining libre-ness, and then recompile the necessary packages.

Expecting an update 24H after reporting something out-of-date is a little unreasonable.

If your security profile is such that your system would be at serious risk from these local exploit CVEs I'd suggest pulling the PKGBUILD and compiling the package locally until the maintainer has a chance to do so.

#2 - 2019-01-14 02:43 AM - lukeshu

Also note that I am reasonably sure that the CFLAGS (-fstack-protection-strong or something) we use protect us from this exploit. I know that is true of Arch, but it is possible that there's a makepkg.conf change we haven't pulled yet.

#3 - 2019-01-15 01:04 AM - eschwartz

Arch used to use -fstack-protector-strong in the default makepkg.conf, however, we have removed it (https://bugs.archlinux.org/task/54736) since beginning with gcc 7.1.1-4 we compiled gcc using --enable-default-ssp, and therefore -fstack-protector-strong is the default even when not specified.

This does not help the systemd case as it must be compiled with -fstack-clash-protection in order to be safe even with an old version of systemd. And to be clear: Arch Linux was vulnerable to these CVEs, until we updated to a new upstream systemd commit.

For more details, the exploit is described here: https://www.qualys.com/2019/01/09/system-down/system-down.txt

The Arch security tracker discusses all four vulnerabilities here:
https://security.archlinux.org/AVG-615
https://security.archlinux.org/AVG-845

(with links to individual CVEs, arch security advisories, and upstream references.)

#4 - 2019-01-19 12:28 AM - bill-auger

systemd v240 is in [libre-testing] if anyone wants to test it out

beware, this is in [libre-testing] for a reason - installing it could break you system - any of you cowboys and cowgals who already have [libre-testing] enabled, do take note

that warning aside, the i686 build seems to be good, but there were issues with other arches - the x86_64 build is most in need of testing ATM

#5 - 2019-01-19 12:53 AM - bill-auger

the latest rebuild for x86_64 made my VM happy again - after a few more users confirm no major problems, we can probably roll this out to [libre] tomorrow

#6 - 2019-01-19 03:27 AM - bill-auger

- Priority changed from bug to wish

- Status changed from open to in progress

- Tracker changed from Bug to Packaging Request

#7 - 2019-01-19 03:47 AM - bill-auger

i686 and x86_64 are in [libre] now - ARM was built and uploaded to libre also (though we really should have tried it in a non-standard repo first) - just waiting to confirm that ARM is viable and we can close this issue (unless someone knows how to build for ppc64le ?)

#8 - 2019-01-20 02:18 AM - bill-auger

- Status changed from in progress to fixed