Packages - Bug #3554

[glibc] Package with CVE not updated upstream, no response upstream.

2023-10-29 06:34 AM - ryry

Status:	not-a-bug	**% Done:**	0%
Priority:	bug		
Assignee:			
Category:			

Description

Hi

Glibc for armv7h has been out of date for well over a year despite x86_64 Arch updating a few times in that space. It has been raised on the arch arm forums, but no responses. This the most recent, https://archlinuxarm.org/forum/viewtopic.php?f=15&t=16624 .

The 2.35 version appears (but please correct me if I am wrong),to be vulnerable to the Looney Tunables: Local Privilege Escalation in the glibc's ld.so (CVE-2023-4911), which was fixed in the updates that both 64 and 32 bit arch got near the beginning of this month.

Is there anything we can do?

ryry

History

#1 - 2023-10-30 12:16 AM - bill-auger

- Status changed from unconfirmed to not-a-bug

many packages depend on glibc very strictly - when the major version of glibc changes, many packages need to be rebuilt; and they all must be held back until they are all ready and can be released simutentously

"no response upstream" is the norm for archlunuxarm - they do not communicate with the community very well - there is not even a bug tracker - that has never caused problems though - but it does cause these long periods of mystery

really, nothing about this is a fixable bug - most widely-used software has CVEs, including glibc 2.38; so upgrading to glibc 2.38 would not fix the "CVE" part - all that remains is "not updated", which is not a bug - the archarm 'glibc' PKGBUILD on github is 2.38; so im sure that they are working on it - otherwise, to ignore glibc for long, would spell the end of a rolling distro

#2 - 2024-02-12 08:50 PM - ryry

I know this got listed as Not-A-Bug, but the version for arm still has the local privilege escalation exploit and it doesn't seem that archlinux arm is going to update this or the toolchain anytime soon. Many people have asked about getting this sorted on their forums, but still no response, despite the PKGBUILDS updating etc. Is there any way that a patch could be applied to a parabola built version of 2.35 without the full rebuild of everything else, like debian/ubuntu/trisquel have done. If it where only just outdated and not a potential vulnerability I wouldn't ask again.

Sorry

Many Thanks
Ry

#3 - 2024-02-12 09:14 PM - bill-auger

glibc comes from archlinuxarm though - ordinarily, an emergency package could be created; but glibc is a special kind of bird - upgrading it alone would break many many other packages - the system probably would not even boot properly - if archlinuxarm has not upgraded it, there must be some set-backs holding up progress - there is no way that i could upgrade glibc in less time than archlinuxarm, unless they are completely ignoring it, which i doubt - it is just unfortunate that they do not communicate well; so there is no way to know how far along the progress is - it could be ready tomorrow - it surely will be someday, or archlinuxarm and parabola's ARM ports are doomed to extinction

#4 - 2024-02-12 09:28 PM - ryry

Thanks for your response and insights on it. As you say, the lack of communication around it and the tool-chain updates from them has meant that nobody can say when etc. I am always hopeful that "todays the day" as there is always that worry regarding it and perhaps the worry that the ARM side of things might suffer.

Once again
Many Thanks