XZ Utils backdoor

Lasse Collin

This page will get updated as I learn more about the incident.

Facts

- CVE-2024-3094
- XZ Utils 5.6.0 and 5.6.1 release tarballs contain a backdoor. These tarballs were created and signed by *Jia Tan*.
- Tarballs created by Jia Tan were signed by him. Any tarballs signed by me were created by me.
- GitHub accounts of both me (Larhzu) and Jia Tan were suspended. Mine was reinstated on 2024-04-02.
- Only I have had access to the main tukaani.org website, git.tukaani.org repositories, and related files. Jia Tan only had access to things hosted on GitHub, including xz.tukaani.org subdomain (and only that subdomain).
- The XZ projects have been moved to their old URLs on tukaani.org. XZ Utils's home page is under construction still though.
- xz.tukaani.org DNS name (CNAME) has been removed and won't be restored.
- The email address xz *at* tukaani *dot* org no longer forwards to Jia Tan. This change was made on 2024-03-30.
- 2024-04-09: The Git repositories of XZ projects are available on GitHub (https://github.com/tukaani-project) again. Please use these for downloading the code to reduce the bandwidth usage on git.tukaani.org.
- GitHub had closed all pull requests and marked them as if I had closed them on 2024-04-05. I didn't close any PRs on that day, GitHub just misattributed it to me. On 2024-04-12 I tried to re-open PRs and GitHub immediately closed them again, again marking them as if I had done it. (On IRC it was suggested that this might have happened because the PRs refer to forks that are disabled.)
- After the primary location of xz.git was officially moved to GitHub, I didn't detected any force pushes to the master or v5.x branches. I haven't force pushed to git.tukaani.org.
- However, I force pushed to the xz-java repository on GitHub on 2024-04-05, deleting two harmless commits by Jia. I had pushed commits to git.tukaani.org when the repositories on GitHub were disabled and I didn't have the two commits by Jia available locally.

- The version 1.0 of the XZ Utils review notes was published on 2024-05-29. (The first work-in-progress version was published on 2024-04-15.)
- New, clean XZ Utils releases were made on 2024-05-29. The home page is available again too.

To media and reporters

I won't reply for now. I might reconsider after my planned article is out.

Email

I have gotten a lot of email. Thanks for the positive comments. Unfortunately I don't have time to reply to most of them.

Donations

A few have suggested that I should enable GitHub Sponsors.

The Finnish law doesn't allow a private person to request money from the general public and give nothing in return. Certain types of organizations can ask for donations but to do that even they need to get a permit first.

This means that things like GitHub Sponsors don't seem legal to use.

Plans

Git repositories

There was discussion if the master branch should have been rebased to purge the malicious files. This would have been equivalent to dropping eight commits (https://git.tukaani.org/?p=xz.git;a=commit;h=e93e13c8b3bec925c56e0c0b675d8000a0f7f754). The main benefit would have been that then antivirus software wouldn't complain about them. Otherwise the files are harmless without the trigger code that was never included in the Git repository.

It was decided that the Git repository will *not* be rebased.

The other Git repositories (xz-embedded and xz-java) are fine and never had malicious or suspicious content.

Releases

There was discussion if the 5.6.x version numbers shouldn't be used further and the next release could be 5.8.0. However, it felt clearer to make XZ Utils 5.6.2 as a cleanup step. There are a few small improvements planned which could become 5.8.0 in shorter time than usual, hopefully replacing 5.6.x somewhat soon.

What can be learned from this

I plan to write an article how the backdoor got into the releases and what can be learned from this.

Links

- Details by Andres Freund (https://www.openwall.com/lists/oss-security/2024/03/29/4)
- FAQ by Sam James (https://gist.github.com/thesamesam/223949d5a074ebc3dce9ee78baad9e27)
- Gentoo bug 928134 (https://bugs.gentoo.org/928134)
- Debian bug 1068024 (https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=1068024)

Last updated 2024-05-29 21:13:00 +0300