THREAT REPORT: XZ Utils Library Vulnerability

April 05, 2024

TLP: WHITE

Executive Summary:

On March 29th, 2024, a secret backdoor (CVE-2024-3094), was discovered in the open source xz-utils package; commonly found in several Linux distributions. This is one of the most sophisticated and well-planned supply chain attacks to date, and had it not been discovered when it was, the xz backdoor may have been rolled out with the stable releases of several Linux distros.

The backdoor specifically enables only the attacker(s) who developed the exploit to establish an encrypted channel between their C2 server and the target. After which, the attacker will have root privilege on the target system. The impacts of a successful exploit will vary, but with such elevated privileges, the attacker could perform any nefarious action they so choose within the system itself.

At the time of writing this, security researchers are still reverse engineering the backdoor and there are still many unknowns. The technical details section outlines relevant background information, the inner workings of the payload, and how organizations can determine if they are affected.

Technical Details

Background:

Xz-utils is a tool that uses the Lempel-Ziv-Markov chain algorithm (LZMA) for lossless compression. It comes stock in most Linux distributions and can be accessed from the terminal using the *xz* command. It additionally contains an API library called liblzma, which many other pieces of software depend on, including the secure shell daemon (sshd). Daemons are autonomous background processes that commonly start at system boot. Sshd is the daemon responsible for running the OpenSSH process and handling related tasks such as authentication, encryption, terminal connections, etc.: an ideal place for a backdoor.

Details:

How does someone compromise an open-source project where everyone can see the code you commit? The way Jia Tan—the open-source contributor who made the backdoor—did it was quite interesting, instead of modifying code in the up-stream source, they modified the release tarballs to contain a series of obfuscated make and binary files masquerading as test files. The payload is in these two files:

1. tests/files/bad-3-corrupt_lzma2.xz
2. tests/files/good-large_compressed.lzma

The first test file decompresses and de-obfuscates the second file, then runs it in /bin/sh. This produces the following injected.txt file from the original post. This file acts as a hook into the build process of liblmza. The attacker uses this to run system checks, some of which are listed here. If the checks pass, the build process is then used to inject an additional file that was previously manipulated by the attacker in 2023. The attacker then uses several techniques to hook the dynamic linker. In doing so, they are able to overwrite the address for a critical RSA decryption function used by sshd, with the address of their exploit code.

Now, whenever the RSA function is used by sshd, it will check for the attackers encrypted and signed ED448 key which they implant into the ssh certificate. If this is detected, the backdoor is activated, and the attacker is granted root level access to the system. In summary, the attacker built a backdoor into the build process of liblmza which hooks the dynamic linker to re-direct the public RSA decrypt function to the attacker's code, which will then run custom backdoor code when, and only when the attacker sends their ssh certificate.

Recommended Actions:

- Identify any Linux based systems and search them for the use of xz 5.6.0 or 5.6.1. These are the versions which contain the backdoor. If these versions of xz-utils are found, they must be rolled back immediately.
    - Hunting queries for Microsoft Defender for Endpoint (MDE)
    - Shell script to detect xz utils version
- Review the tables of affected Linux distributions of affected and unaffected Linux distributions and prioritize the affected distributions if they are in your environment.
- The Cybersecurity and Infrastructure Security Agency (CISA) advises that organizations rollback to unaffected versions such as xz Utils 5.4.6.

Further Reading:

- Red Hat warns of backdoor in XZ tools used by most Linux distros | BleepingComputer
- xz-utils backdoor situation | github.com
- xzbot backddor demo | github.com
- original post | openwall.com

CYBER ALBERTA

Disclaimer