INFORMATION NOTE

→ 03/04/2024

DISCOVERY OF A BACKDOOR IN XZ UTILS

On March 29 2024, Andres Freund, a developer working at Microsoft disclosed **the presence of a backdoor in XZ Utils targeting the most important security infrastructure of the internet**. XZ Utils is an open source data compression tool available on almost all installations of Linux distributions. Web developers host their websites and apps on Linux. Linux comes with OpenSSH to make site administration easier. All you need to do to gain access anywhere is to wait for the most recent version of XZ to be included in Linux by creating a backdoor into it.

CVE-2024-3094 was rated with the highest possible score (CVSS score: 10.0). **It allows attackers to** send payloads through an SSH certificate to **bypass authentication** and **gain control over the victim's machine**.

The malicious code was intentionally introduced by a GitHub member known as Jia Tan who joined the project in 2022 as a new maintainer. According to researchers, **this operation could be conducted by state-sponsored actors to be used multiple times for years.** However, the project was initially launched by Lasse Collins who decided to hand over the project to Jia Tan. **The repository was disabled**.

HOW DOES IT WORK?

Versions 5.6.0 and 5.6.1 of XZ Utils contained malicious code that altered the program's functionality when handling.lzma compression and decompression operations. These SSH-related routines made it possible for malicious programs to run with root access. With the help of this code, a user with the pre-encryption key could access the backdoored system via SSH. That individual would then possess the same degree of authority as any other approved administrator.

RECOMMENDATIONS

- Determine which of your network's systems might be vulnerable.
- Apply the protection measures suggested by the application or OS publisher.

RESSOURCES

- https://lists.debian.org/debian-security-announce/2024/msg00057.html
- https://www.redhat.com/en/blog/urgent-security-alert-fedora-41-and-rawhide-users
- https://news.opensuse.org/2024/03/29/xz-backdoor/
- https://archlinux.org/news/the-xz-package-has-been-backdoored/

REFERENCES

CISA. 2024. Reported Supply Chain Compromise Affecting XZ Utils Data Compression Library, CVE-2024-3099. https://cisa.gov/news-events/alerts/2024/03/29/reported-supply-chain-compromise-affecting-xz-utils-data-compression-library-cve-2024-3094

Dan Goodin. 2024. Wired. The XZ Backdoor: Everything You Need to Know. https://www.wired.com/story/xz-backdoor-everything-you-need-to-know/

Debian Security. 2024. Xz-utils security update. https://lists.debian.org/debian-security-announce/2024/msg00057.html

Meissner, Marcus. 2024. openSUSE addresses supply chain attack against xz compression library. https://news.opensuse.org/2024/03/29/xz-backdoor/

RedHat. 2024. Urgent security alert for Fedora Linux 40 and Fedora Rawhide users. https://www.redhat.com/en/blog/urgent-security-alert-fedora-41-and-rawhide-users

Runge, David. 2024. Archlinux. The xz package has been backdoored. https://archlinux.org/news/the-xz-package-has-been-backdoored/

The Hacker News. 2024. Malicious Code in XZ Utils for Linux Systems Enables Remote Code Execution. https://thehackernews.com/2024/04/malicious-code-in-xz-utils-for-linux.html