ultraviolet

CONFIDENTIAL

THREAT REPORT:

XZ: What Happened and Why

Services Performed By:
UltraViolet Cyber
Peter Cipolone
(443) 351-7630
info@uvcyber.com

Published Date:
April 17, 2024

Contents

1 Executive Summary

A software engineer from Microsoft was troubleshooting slow SSH logins and ended up finding malware. The malware, found in Linux utility xz/liblzma, was a backdoor which allowed for unauthorized remote access of Linux systems. This backdoor was implemented by a new, mysterious, maintainer of xz, an opensource compression tool. Since the backdoor was caught early on, only the versions of xz/liblzma are 5.6.0 and 5.6.1 are affected. Currently, only cutting-edge versions of major Linux distros are vulnerable.

2 Technical Analysis

In a Hollywood-styled cybersecurity caper, a software engineer accidentally uncovered a cybersecurity attack that was years in the making. Labeled CVE-2024-3094, this vulnerability is an SSH backdoor in the opensource Linux utility xz/liblzma which allows for remote code execution and compromise of Linux servers. Software Engineer Andres Freund was investigating slow SSH login times traced the backdoor to xz, a dependency of OpenSSH.

An ongoing investigation has revealed that the backdoor appears to have been created by project maintainer Jia Tan, who might not be a real person. The current attack timeline shows that Jia Tan appeared out of thin air sometime in 2021 and started making contributions to the xz project. After a couple of years of contributions and the help of some sock puppet accounts, Jia is given permission to help maintain the project. Once a maintainer, the backdoor code is added to the project and begins to be pushed out to different Linux distros. The rollout was just beginning when it was discovered by Andres Freund. This attack has the hallmarks of a nation state actor, but no attribution has been made.

Since the investigation into the XZ backdoor is ongoing, the details surrounding the vulnerability are slim and inconsistent. However, it appears that the backdoored code targeted decryption routines in OpenSSH and allowed attackers with a specific key to execute code before the authentication step, effectively bypassing it. With the discovery coming so early in the rollout process, only the cutting-edge versions of Linux distributions appear to be impacted. If a system meets the following conditions, it is advised to downgrade the XZ utility to an uncompromised version.

- Using a .deb or .rpm based distro with glibc and xz-5.6.0 or xz-5.6.1
- Using another type of distribution with glibc and xz-5.6.0 or xz-5.6.1

3 What UltraViolet Cyber is Doing

- UltraViolet Cyber regularly updates our IOC database to ensure alerting is up to date
- Monitoring commands that are associated with malicious activity from threat actors
- Monitoring network logs for traffic to known malicious sites

4 What Customers Can Do

- Identify any systems that have xz-5.6.0 or xz-5.6.1 installed and downgrade to a non-compromised version.
- Keep abreast of the situation and respond to any new revelations of the investigation.

5 References

- Boehs, Evan. Everything I Know about the XZ Backdoor, 29 Mar. 2024, boehs.org/node/everything-i-know-about-the-xz-backdoor.
- Freund, Andres. “Oss-Security - Backdoor in Upstream XZ/Liblzma Leading to SSH Server Compromise.” Openwall, www.openwall.com/lists/oss-security/2024/03/29/4. Accessed 7 Apr. 2024.
- James, Sam. “XZ-Utils Backdoor Situation (CVE-2024-3094).” Gist, gist.github.com/thesamesam/223949d5a074ebc3dce9ee78baad9e27. Accessed 8 Apr. 2024.
- Lcamtuf. “Techies vs Spies: The XZ Backdoor Debate.” Techies vs Spies: The Xz Backdoor Debate, lcamtuf’s thing, 30 Mar. 2024, lcamtuf.substack.com/p/technologist-vs-spy-the-xz-backdoor.
- Menashe, Shachar, et al. “XZ Backdoor Attack CVE-2024-3094: All You Need to Know.” JFrog, 7 Apr. 2024, jfrog.com/blog/xz-backdoor-attack-cve-2024-3094-all-you-need-to-know/.