CS7NS5 Security and Privacy
AS2 Security or privacy incident

Ted Johnson
School of Computer Science and Statistics
Trinity College Dublin

19 April 2024

A Short Case Study on Supply Chain Attacks

In only the last couple of weeks, there has been a number of major security and privacy incident revelations. Of particular note have been the OS command injection vulnerability found in GlobalProtect, the GoFetch side-channel attack against Apple M1 CPUs, and the eavesdropping of SSL traffic orchestrated by Facebook against users of competitor services though Project Ghostbusters [1–3]. We have also seen a use-after-free bug in Linux kernel exploited to perform privilege escalation with CVE-2024-1086 as well as a key recovery leak on the PuTTY SSH and Telnet client [4, 5]. However, I believe the discovery of a backdoor installed within the XZ Utils project is the most significant recent incident in the field and provides a valuable example of how supply chain attacks pose a serious risk to the security of digital systems and organisations [6].

In March 2024, the software developer Andres Freund observed a measurable decrease in the performance of OpenSSH login connections under certain circumstances. During investigation, he was able to isolate the cause to be with the lzma data compression library of XZ Utils, which is commonly patched into OpenSSH by Linux distributions that use systemd. After analysis of the open source software, Freund discovered malicious code had been inserted into the project to allow for the bypass of the OpenSSH authentication mechanisms. He reported these findings to Debian and the distros@openwall mailing list on the 28th of March, where the exploit was quickly confirmed and subsequently urgent security advisories were published by the following day [7, 8].

This exploit was the result of an elaborate scheme executed over a number of years by an unknown individual or organisation identifying themselves as Jia Tan. Beginning in late 2021, Tan becomes a frequent contributor to XZ Utils, submitting several legitimate patches through the xz-devel mailing list. Pressured by emails demanding an increase in productivity

likely originating from false personas operated by the same threat actor, the sole project maintainer Lasse Collin is eventually convinced to grant Tan maintainership status with direct commit permission by the end of 2022 [9]. Having now gained enough trust from Collin and control over the project, Tan is able to subtlety adjust the codebase across a series of innocuous changes to accommodate the planned vulnerability, which is finally installed on the 23rd of February 2024 as a mechanism to inject malicious code concealed inside two binary testing files into the OpenSSH `sshd` process [10]. This backdoor substitutes the OpenSSH `RSA_public_decrypt` function with a version that allows for an attacker in possession of a specific private key to circumvent SSH authentication and thus gain root access to all compromised systems remotely.

As a smaller project regularly depended on by the ubiquitously used OpenSSH, the covert insertion of this exploit into XZ Utils is a prime example of a supply chain attack, and had the potential to affect hundreds of millions of devices, including many highly critical and sensitive targets. Thankfully, in this case Freund was able to detect and expose this backdoor before it had seen widespread deployment amongst production systems through a new stable Linux distribution release. This event has highlighted both the inherent but often neglected risk introduced to digital infrastructure through software dependencies as well as the importance to security for anyone to be able to freely audit the software they use by following an open source development model.

References

[1] *CVE-2024-3400*. Available from National Vulnerability Database. Apr. 2024. URL: https://nvd.nist.gov/vuln/detail/CVE-2024-3400 (visited on 04/19/2024).

[2] Boru Chen et al. "GoFetch: Breaking Constant-Time Cryptographic Implementations Using Data Memory-Dependent Prefetchers". In: *USENIX Security*. 2024.

[3] *Klein v. Meta Platforms, Inc., No. 3:20-cv-08570-JD*. United States District Court, Northern District of California. Aug. 2022.

[4] *CVE-2024-1086*. Available from National Vulnerability Database. Jan. 2024. URL: https://nvd.nist.gov/vuln/detail/CVE-2024-1086 (visited on 04/19/2024).

[5] *CVE-2024-31497*. Available from National Vulnerability Database. Apr. 2024. URL: https://nvd.nist.gov/vuln/detail/CVE-2024-31497 (visited on 04/19/2024).

[6] *CVE-2024-3094*. Available from National Vulnerability Database. Mar. 2024. URL: https://nvd.nist.gov/vuln/detail/CVE-2024-3094 (visited on 04/19/2024).

[7] Andres Freund. *backdoor in upstream xz/liblzma leading to ssh server compromise*. oss-security mailing list archive. Mar. 2024. URL: https://lwn.net/ml/oss-security/20240329155126.kjjfduxw2yrlxgzm@awork3.anarazel.de/ (visited on 04/19/2024).

[8] Jonathan Corbet. *A backdoor in xz*. LWM.net. Mar. 2024. URL: https://lwn.net/Articles/967180 (visited on 04/19/2024).

[9] Lasse Collin. *Re: [xz-devel] XZ for Java*. xz-devel mailing list archive. May 2022. URL: https://www.mail-archive.com/xz-devel@tukaani.org/msg00563.html (visited on 04/19/2024).

[10] Jia Tan. *Commit cf44e4b "Tests: Add a few test files."* git.tukaani.org. Feb. 2024. URL: https://git.tukaani.org/?p=xz.git;a=commitdiff;h=cf44e4b7f5dfdbf8c78aef377c10f71e274f63c0 (visited on 04/19/2024).