CS7NS5 Security and Privacy
AS2 Security or privacy incident

Ted Johnson
School of Computer Science and Statistics
Trinity College Dublin

19 April 2024

On The Threat of 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 firewall devices, the GoFetch side-channel attack against Apple M1 CPUs, and the interception and decryption 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, <xz utils was big>

On the <andreas notices performance effect in latest release, investigation and discovery>. [6] [7] [8]

<this was the result of a long and elaborate scheme executed through an identify to install a backdoor in the project>. <history of the attack>

<effect of the backdoor (dependencies aka a supply chain attack)>

<countermeasures and the benefit of the many eyes in open source software - caught early before entering production systems>

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).