Threat Intelligence Report

XZ Utils Supply Chain Attack Highlights Pitfalls of Open-Source Software Dependencies

Open-source code is ubiquitous in today's applications – one study of commercial codebases across 17 industries found that 96% contained open-source code. Open-source software projects often claim to be secure, as the source code is publicly available for audit and regularly evaluated by contributors. However, in March 2024 a researcher discovered a vulnerability in XZ Utils, an open-source data compression utility present on nearly all installations of Linux and other Unix-like operating systems. The code manipulation appeared to be an intentional modification, resulting in a vulnerability that NIST assigned the highest-possible severity score of 10.0.[1] This vulnerability can result in unauthorized remote access under certain conditions and was likely purposefully crafted by a trusted developer over several years, highlighting the opportunity open-source software presents to threat actors committed to the long-term planning of their attacks.

THREAT ACTIVITY

- Using the alias Jia Tan, the threat actor responsible for the XZ Utils backdoor began contributing to open-source software projects on GitHub in 2021, and gained "commit access," or the ability to modify the code repository, to XZ Utils in January 2023, eventually achieving release manager rights. Jia Tan became increasingly involved in the XZ Utils utility, adding modifications which laid the groundwork for eventual implementation of the backdoor. This included requesting that "oss-fuzz," a project that scans open-source software for vulnerabilities, disable a particular function during testing, preventing "oss-fuzz" from detecting the malicious changes made to XZ Utils.
- In February 2024, Jia Tan successfully implemented this backdoor in two iterations. In version 5.6.0, the threat actor added code to the XZ repository enabling injection of the backdoor on Debian and Fedora distributions.2 Version 5.6.1 introduced the ability to execute additional shell scripts during the build phase. This phased approach was likely intentional to make future updates to the backdoor less suspicious.
- Following the implementation of the backdoor, Jia Tan appealed to the developers of the Ubuntu, Red Hat, and Debian distributions to merge the updates into their operating systems. If not for a single researcher discovering the backdoor, this merge would have likely occurred, significantly expanding the reach of potential supply chain compromises.

THREAT ASSESSMENT

- The decentralized responsibility for maintaining open-source software leaves space for abnormalities to be missed or overlooked, increasing vulnerabilities and risks.
- Threat actors are likely to target widely-used open-source libraries to reach the maximum number of potential victims. This includes infiltrating third parties and leveraging that access to gain entry to connected entities.
- While open-source software is perhaps easier for threat actors to access and manipulate, threat actors may seek to deploy similar long-term social engineering tactics against software development vendors to infect closed-source components, which are not available for public scrutiny and analysis.

RECOMMENDED ACTION

- Identify open-source dependencies and those of key vendors: create and maintain a Software Bill of Materials (SBOM) that inventories open-source components.
- Plan for supply chain compromises in your Incident Response Plan (IRP).
- Ensure you are up-to-date on the latest cyber threat intelligence related to critical vulnerabilities, malicious code, or other security risks associated with open-source software.
- Maintain vigilance when using open-source software and patch as updates become available.
- Use automated security testing (e.g., scanning software for vulnerabilities with an automated tool) to identify and mitigate software security issues with open-source code.

Footnotes:

[1] CVE-2024-3094

[2] Linux distribution systems compile code from various open-source projects and combine it into a single operating system that can be installed and booted up. Some of these distributions are entirely community-driven, while others are commercially backed.

SOURCES

Sources include open-source information from public and private industry reporting.

- Intel Profile Detail - Microsoft Defender
- GitHub - About commits
- The XZ Backdoor: Everything You Need to Know
- Reported Supply Chain Compromise Affecting XZ Utils Data Compression Library, CVE-2024-3094
- Why open-source software supply chain attacks have tripled in a year
- XZ Utils Backdoor | Threat Actor Planned to Inject Further Vulnerabilities
- 2024 Open Source Security and Risk Analysis Report

Why FTI Cybersecurity

Multidisciplinary Expertise

Intelligence-led, expert-driven, strategic approach to cybersecurity challenges

Core team from intelligence agencies, law enforcement, prosecuting offices, and global private sector institutions

Globally Positioned

Ability to respond anywhere in the world

Ability to staff the largest and most complex engagements and investigations

Relationships with the top global intelligence agencies, regulatory authorities, and private agencies

Integrated & Comprehensive

Comprehensive services include crisis communications, e-discovery, forensic investigations, and more

Seamless integration of FTI Consulting's expertise across service offerings

FTI Cybersecurity Global Offices

Americas

Atlanta
Boston
Chicago
Dallas
Houston
Irvine
Los Angeles
Mexico City
Miami
New York
Philadelphia
Roseland
San Francisco
Sao Paulo
Seattle
Toronto
Washington, DC
Wayne

EMEA

Berlin
Brussels
Cape Town
Dubai
Dublin
Dusseldorf
Frankfurt
Johannesburg
London
Madrid
Mumbai
Munich
Paris
Zurich

APAC

Brisbane
Hong Kong
Melbourne
Perth
Shanghai
Singapore
Sydney
Tokyo

CONTACT FTI CYBERSECURITY

Email: #fticybersecurity@fticonsulting.com

Phone: +1-844-CYBR-FTI (+1-844-292-7384)