Smarttech
YOUR 24/7 SECURITY PARTNER

Cyber Threat Intelligence Report

XZ Utils Backdoor: Impact on Major Linux Distributions

NSAI

INFORMATION SECURITY
NSAI Certified

QUALITY
NSAI Certified

www.smarttech247.com

Contents

Introduction

This document is prepared as a part of the latest threat intelligence research conducted by the Smarttech247 team. This report delves into a significant supply chain threat affecting major Linux distributions through compromised versions of the XZ Utils data compression library. This threat has raised alarms within the cybersecurity community due to its sophisticated nature and far-reaching implications. By examining the discovery, impact, response efforts, and implications for the industry, this report aims to provide a comprehensive understanding of the attack.

Methodology

This report presents proprietary rising cyber threat data and research from the Smarttech247.

All the facts and statements about to be presented are gathered based on the information that the Smarttech247 team collects as part of its threat intelligence department.

Discovery and Impact

In a recent highly sophisticated cyber operation, threat actors stealthily implanted a backdoor within a Linux operating system package. The backdoor could potentially enable threat actors to gain remote access to vulnerable systems. The backdoor was discovered on March 29th within the XZ Utils package versions 5.6.0 and 5.6.1; the package is being utilised for data compression in Linux environments.

This operation also provides the threat actor with a potential vector to perform remote code execution (RCE) with system privileges over vulnerable systems, posing a risk of unauthorised access and system compromise.

Red Hat's advisory underscored the severity of the situation, urging users to cease usage of affected systems and revert to safe versions of XZ Utils. This serves as a wake-up call for organisations to prioritize security hygiene and implement robust security

measures to mitigate the risk of supply chain attacks. Additionally, this emphasises the importance of timely communication and collaboration within the Linux community to address emerging security threats effectively.

Debian and Ubuntu promptly addressed the issue, ensuring that stable releases remained unaffected by the compromised packages. However, testing, unstable, and experimental distributions were impacted, prompting immediate remediation measures to mitigate the risk of further exploitation.

Binarly's release of XZ.fail provided a valuable resource for the security community, offering a comprehensive and reliable means of detecting the XZ Utils backdoor.

Technical Details of the Attack

The attack mechanism leveraged complex obfuscations within the liblzma build process, facilitating the insertion of malicious code designed to intercept and modify data interactions. This manipulation targeted critical authentication protocols, particularly in sshd via systemd, compromising the integrity of remote access mechanisms. The sophistication of the attack highlighted the adversaries' advanced capabilities and underscored the need for enhanced security measures to detect and mitigate such threats.

Affected Linux Distributions

Several prominent Linux distributions, including Fedora Rawhide, Fedora Linux 40 beta, openSUSE Tumbleweed, openSUSE MicroOS, Kali Linux, and Arch Linux, were confirmed to have been impacted by the supply chain attack. However, Debian and Ubuntu remained unscathed, with stable releases unaffected by the compromised packages. The selective targeting of distributions raised questions about the attackers' motives and the potential scope of the breach.

Response and Mitigation Efforts

In response to the attack, various stakeholders, including Red Hat and Debian, issued advisories urging users to downgrade to uncompromised versions of XZ Utils and conduct thorough system scans for potential malicious activity. Additionally, Binarly released XZ.fail, a free backdoor detection tool, to assist in identifying compromised

binaries and safeguarding against further exploitation. The coordinated response efforts demonstrated the importance of community collaboration and proactive security measures in mitigating supply chain attacks.

Detection Tools and Methods

Existing detection methods, primarily focused on version checks and hash-based analysis, proved insufficient in accurately identifying the XZ Utils backdoor, leading to potential false positives. Binarly's approach, utilising behavioural analysis and static analysis of control flow graph transitions, offered a more effective and accurate means of detecting the backdoor implantation. The tool's low false-positive rate and generic detection capabilities enhanced its utility in safeguarding against similar threats and underscored the importance of innovative detection techniques in combating evolving cyber threats.

Analysis of the Backdoor

The complexity and sophistication of the XZ Utils backdoor, including its utilisation of GNU Indirect Function attributes and multi-stage loading, highlighted its orchestrated nature and the level of planning involved. Furthermore, the involvement of XZ Utils' maintainer, Jia Tan, raised questions about project security and oversight, emphasizing the need for enhanced governance and accountability within open-source communities.

One of the core techniques used by the XZ backdoor to gain initial control during execution is the GNU Indirect Function (ifunc) attribute for the GCC compiler to resolve indirect function calls in runtime. The implanted backdoor code initially intercepts or hooks execution. It modifies ifunc calls to replace a check "is_arch_extension_supported" which should simply invoke "cpuid" to insert a call to "_get_cpuid" which is exported by the payload object file (i.e., liblzma_la-crc64-fast.o) and which calls malformed _get_cpuid() which is implanted into the code shown in the figure below.

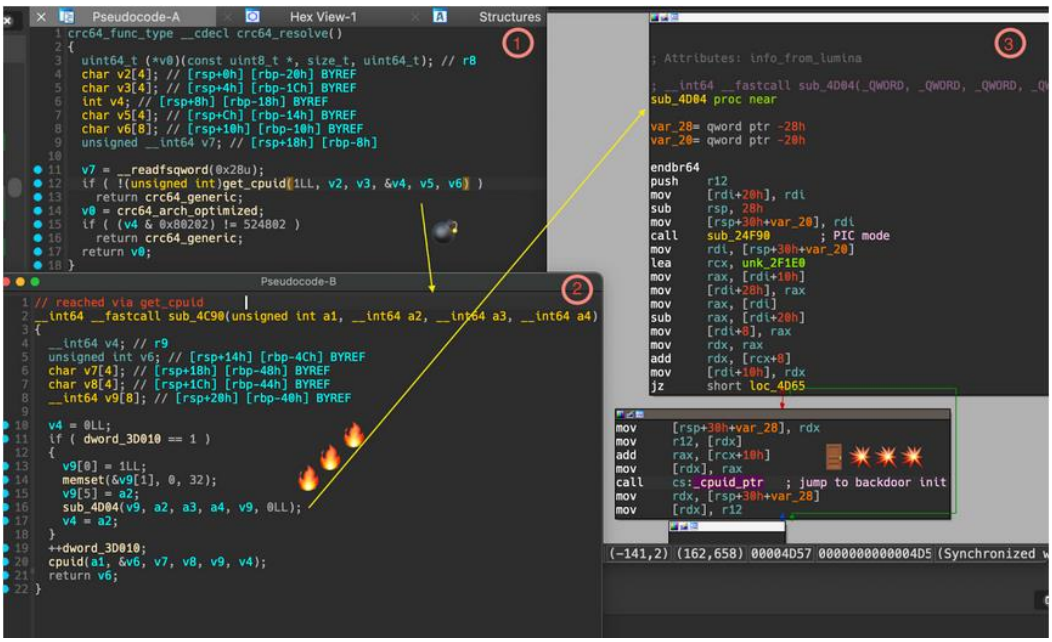

Fig. 1 Code execution

Source: https://www.binarly.io/blog/xz-utils-supply-chain-puzzle-binarly-ships-free-scanner-for-cve-2024-3094-backdoor

CVE-2024-3094

The vulnerability CVE-2024-3094, discovered within the XZ Utils data compression library, represents a critical security flaw that has impacted major Linux distributions. This vulnerability stems from the insertion of malicious code into the library's upstream tarballs, starting with version 5.6.0.

Risk Information:

VPR

- Risk Factor: Critical
- Score: 10.0

CVSS v2

- Risk Factor: Critical
- Base Score: 10
- Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

The exploitation of this vulnerability underscores the persistent threat posed by supply chain attacks and highlights the importance of proactive security measures to mitigate such risks effectively.

Implications for the Industry

The XZ Utils supply chain attack served as a stark reminder of the pervasive nature of supply chain attacks and underscored the need for enhanced security measures across the software supply chain. The threat highlighted the importance of proactive threat detection and mitigation strategies and emphasised the need for robust governance and accountability within open-source communities. Moving forward, organisations must prioritise security hygiene and implement comprehensive security measures to safeguard against emerging cyber threats effectively.

Recommendations

- XZ Utils users should downgrade to an older version of the utility immediately (i.e., any version before 5.6.0) and update their installations and packages according to distribution maintainer directions.
- Apply the Principle of Least Privilege to all systems and services. Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack
- Conduct vulnerability scanning to find potentially exploitable software vulnerabilities
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources. Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources

IOCs

File names:

257fc477b9684863e0822cbad3606d76c039be8dd51cdc13b73e74e93d7b04cc.elf

liblzma_la-crc64-fast.o

MD5

a78380f647766a2bc099844375bd5a4c

212ffa0b24bb7d749532425a46764433

SHA-1

4546876d037d899090260fcf9fe49683998cc9de

0ebf4b63737cdf3e084941c7d02f8eec5ca8d257

SHA-256

257fc477b9684863e0822cbad3606d76c039be8dd51cdc13b73e74e93d7b04cc

cbeef92e67bf41ca9c015557d81f39adaba67ca9fb3574139754999030b83537

References

https://www.securityweek.com/supply-chain-attack-major-linux-distributions-impacted-by-xz-utils-backdoor/

https://securityaffairs.com/161396/security/cve-2024-3094-backdoor-scanner.html

https://www.cve.org/CVERecord?id=CVE-2024-3094

https://securityaffairs.com/161224/malware/backdoor-xz-tools-linux-distros.html

https://www.cisa.gov/news-events/alerts/2024/03/29/reported-supply-chain-compromise-affecting-xz-utils-data-compression-library-cve-2024-3094

https://www.redhat.com/en/blog/urgent-security-alert-fedora-41-and-rawhide-users

https://www.binarly.io/blog/xz-utils-supply-chain-puzzle-binarly-ships-free-scanner-for-cve-2024-3094-backdoor

https://github.com/FabioBaroni/CVE-2024-3094-checker