Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

XZ Utils Backdoored, A Supply Chain Nightmare For Linux Distros

Date of Publication	Admiralty Code	TA Number
April 1, 2024	A1	TA2024124

Summary

Discovered On: March 29, 2024
Affected Products: Fedora and Other Linux Distros
Impact: Multiple Linux distributions face a potential supply chain threat due to the introduction of malicious code into a widely-used library across most distributions. A backdoor was discovered within the XZ Utils library, inserted roughly a month ago. This compromise allows attackers to manipulate and intercept data exchanged by software routines that rely on XZ Utils as a dependency.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2024-3094	XZ Utils Embedded Malicious code	XZ Utils	✗	✗	✗

Vulnerability Details

#1 The XZ library has been compromised by a backdoor, which was surreptitiously inserted into its source code. This infiltration, originating from one of the maintainer's accounts, poses a significant threat to numerous Linux distributions that rely on this library.

#2 The discovery of the backdoor occurred during the investigation of SSH performance issues, raising concerns about its potential presence within Linux distributions. The malicious code, if present, could facilitate unauthorized access to affected systems, posing a serious security risk.

#3 XZ is a widely-used data compression technique, similar to gzip, found in virtually all Linux distributions. XZ Utils serves as a command line tool for enabling XZ compression and decompression. Additionally, liblzma provides an API for data compression.

#4 The malicious code intricately alters functions within the liblzma codebase, which is integral to the XZ Utils package. The result is a tampered liblzma library, which may serve as a dependency for various software, granting attackers the ability to intercept and manipulate data exchanges via this library.

#5 This backdoor code poses a critical threat, especially given its impact on SSH authentication mechanisms, potentially enabling unauthorized access to affected systems. It primarily impacts Fedora Systems and Debian, while RHEL systems remain unaffected. It also affects multiple package managers like Homebrew, and a comprehensive evaluation of other affected software and systems is ongoing.

#6 The timely discovery of this backdoor has averted significant supply chain disruptions. Given that the first infected version was released in the final week of February, many software components have not yet integrated it, thus limiting its real-world impact to a considerable extent.

#7 Considering the sophistication of attackers and the extensive potential impact, it is strongly advised to assess the impact within your environment promptly. Additionally, it is recommended to downgrade XZ Utils to an uncompromised version, such as XZ Utils 5.4.6, and conduct thorough investigations to detect any signs of malicious activity.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-3094	XZ Utils or liblzma Versions 5.6.0, 5.6.1 Fedora : Versions 40, 41(Rawhide)	cpe:2.3:a:tukaani:xz-utils:*:*:*:*:*:*:*:*	CWE-506

Recommendations

Assess Impact: Conduct a thorough assessment within your environment to verify whether any instances of the affected version of XZ Utils are in use. Pay special attention to unreleased or trial software components, as they may inadvertently incorporate the compromised version.

Downgrade Version & Limit Service Exposure: Downgrade XZ Utils to a stable version before 5.6.0, such as XZ Utils 5.4.6. SSH daemon is currently known to be affected, consider limiting SSH service exposure to limited network areas.

Vulnerability Management: Implement a robust vulnerability management process to ensure that software and systems are regularly assessed for vulnerabilities and updated with the required security patches. Prioritize critical vulnerabilities identified by security advisories and vendors to mitigate the risk of exploitation by threat actors.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	T1195 Supply Chain Compromise
T1195.001 Compromise Software Dependencies and Development Tools	T1650 Acquire Infrastructure	T1608 Stage Capabilities	

Indicator of Compromise (IOCs)

TYPE	VALUE
MD5	4f0cf1d2a2d44b75079b3ea5ed28fe54, d26cefd934b33b174a795760fc79e6b5, d302c6cb2fa1c03c710fa5285651530f, 53d82bb511b71a5d4794cf2d8a2072c1, 212ffa0b24bb7d749532425a46764433, d26cefd934b33b174a795760fc79e6b5, 540c665dfcd4e5cfba5b72b4787fec4f, 35028f4b5c6673d6f2e1a80f02944fb2, 4ec47410372386d02c432ba10e5d7fda, 079d41f2e76288f1fdd65e72bf58c304

Workaround

Downgrade XZ Utils to a stable version before 5.6.0, such as XZ Utils 5.4.6

References

https://openwall.com/lists/oss-security/2024/03/29/4

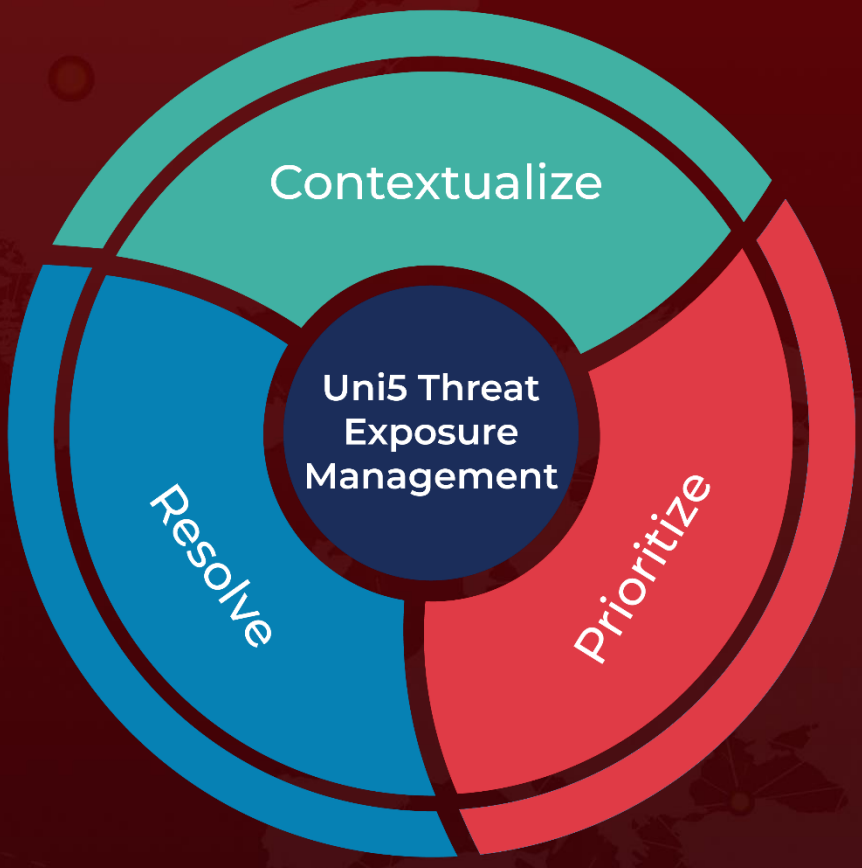
https://www.tenable.com/blog/frequently-asked-questions-cve-2024-3094-supply-chain-backdoor-in-xz-utils

https://sysdig.com/blog/cve-2024-3094-detecting-the-sshd-backdoor-in-xz-utils/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

April 1, 2024 • 8:00 AM

More at www.hivepro.com