SECURITYBOAT
Frontline Of Your Business

XZ-UTILS BACKDOOR
(CVE-2024-3094)
HANDBOOK

www.securityboat.net

SECURITYBOAT
Frontline Of Your Business

Table of contents

1. Background Information

1.1 What is XZ-utils?

XZ-Utils is a set of free, open-source command-line utilities for compressing and decompressing files using the LZMA (Lempel-Ziv-Markov Chain-Algorithm) compression algorithm. It provides high compression ratios and fast decompression speeds, making it suitable for archiving and distributing files.

1.2 What is ifunc?

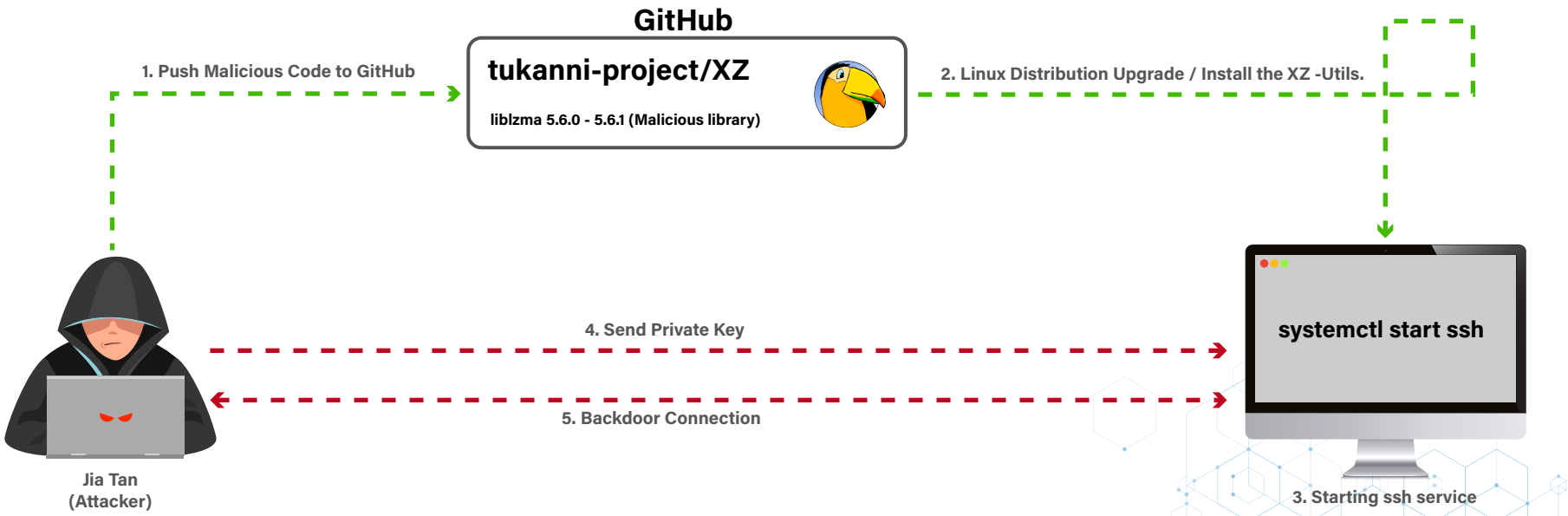
ifunc in GNU allows you to choose which function to use at runtime, rather than at compile time. It's handy when you want your program to adapt dynamically to different situations, such as different CPU types or features.

1.3 What is CRC64?

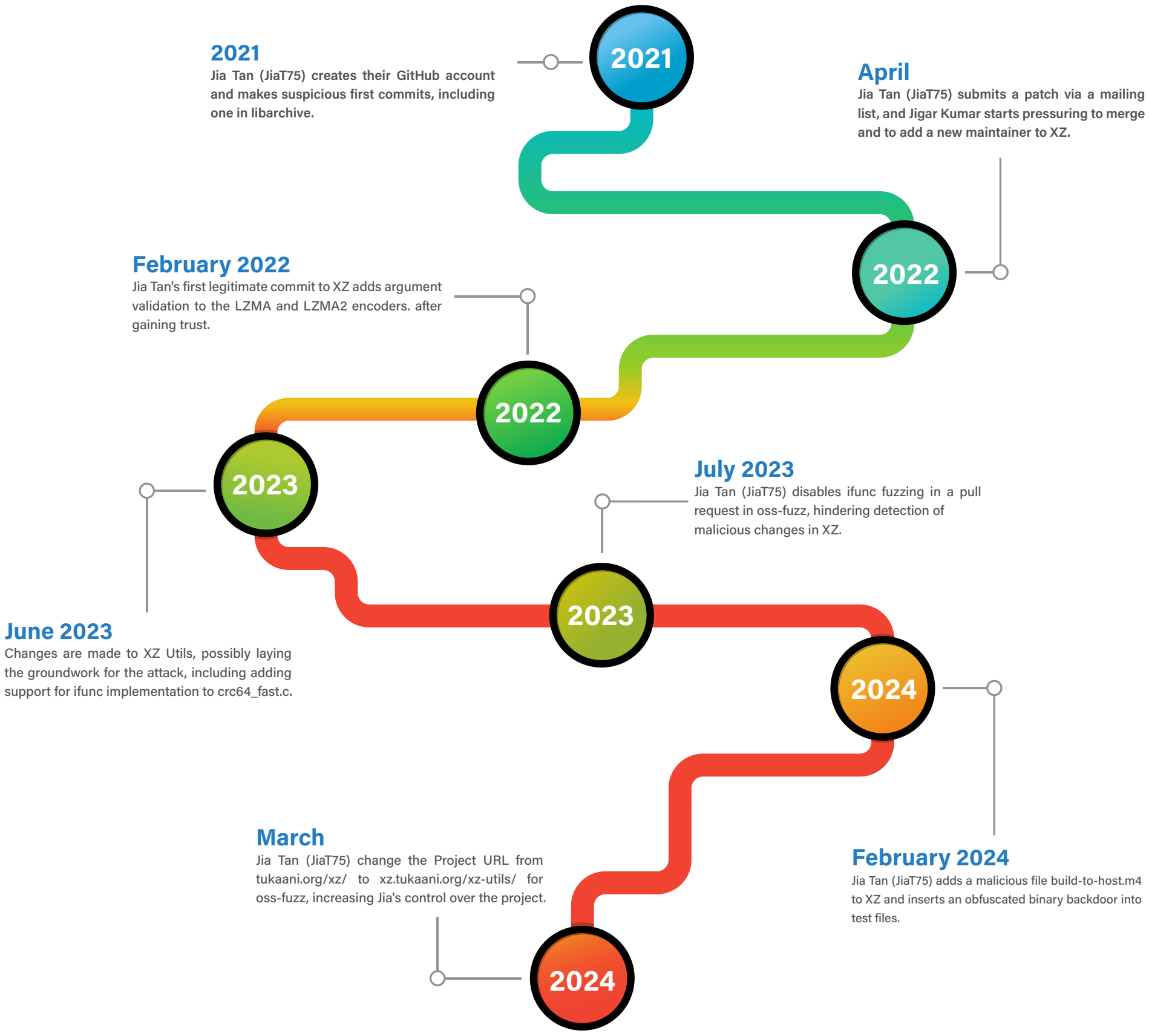
CRC64 (Cyclic Redundancy Check 64) is a checksum algorithm utilized to detect errors in data transmission or storage by calculating a 64-bit value based on data content. This value is appended to the data for verification, ensuring data integrity in networks, storage systems, and communication protocols.

2. What is XZ-Utils Backdoor (CVE-2024-3094)

The XZ Utils backdoor is a vulnerability inserted into the XZ Utils, an open-source data compression utility widely used in Linux and Unix-like operating systems. Planted within the liblzma library in versions 5.6.0 and 5.6.1, this backdoor allows attackers with a specific Ed448 private key to execute remote code on affected Linux systems. The malicious code alters the software's behavior during lzma compression or decompression operations involving SSH, granting attackers root privileges.



3. The Beginnings of XZ-Utils Backdoor



4. Condition for Attack

- The Victim should be running .deb or .rpm based distro with glibc (for IFUNC).
- The Victim should be running either version 5.6.0 or 5.6.1 of xz or liblzma installed. Note that xz-utils provides the liblzma library.
- The Victim should be running systemd with SSH accessible publicly.

5. How to Detect this Vulnerability

5.1 Command to check XZ Versions

Execute the following command to reveal the version of xz present on your system. If the version is either “5.6.0” or “5.6.1”, there’s a possibility that your system could be susceptible to CVE-2024-3094.

```
xz --version
```

5.2 Script for detecting vulnerable XZ via hexdump

This script searches for a specific function signature in the liblzma library utilized by sshd. If this function signature is present, it suggests that the library may be compromised, and the script will indicate that your system is likely vulnerable.

```
#! /bin/bash
set -eu
# find path to liblzma used by sshd
path="$(ldd $(which sshd) | grep liblzma | grep -o '/[^ ]*')"
# does it even exist?
if [ "$path" == "" ]
then
        echo probably not vulnerable
        exit
fi
# check for function signature
if hexdump -ve '1/1 "%.2x"' "$path" | grep -q f30f1efa554889f54c89ce5389fb81e7000000804883ec28488954241848894c2410
then
        echo probably vulnerable
else
        echo probably not vulnerable
fi
```

5.3 Script for detecting CVE-2024-3094

This script checks for potential vulnerability to CVE-2024-3094 by performing two checks. Firstly, it statically checks for a malicious version of xz or liblzma library without executing the xz binary. Secondly, it verifies if the installed SSH server (sshd) utilizes the liblzma library. If both conditions are met, indicating a compromised library and its usage by sshd, the script concludes that the system is likely vulnerable to CVE-2024-3094.

Script:

https://github.com/jfrog/cve-2024-3094-tools/blob/main/cve-2024-3094-detector/cve-2024-3094-detector.sh

6. How XZ-utils backdoor works

1 — Code Injection into XZ Tarballs

The payload is inserted into the source tree during the build process. The affected files include tests/files/bad3corrupt_lzma2.xz and tests/files/goodlarge_compressed.lzma.

2 — Object File Extraction

A disguised test file within the liblzma build process yields a prebuilt object file. This object file contains modified functions introducing the backdoor functionality.

3 — Incorporation into SSH (sshd)

The manipulated liblzma library, now containing the backdoor, integrates into the sshd executable. When the backdoored XZ library loads via a /usr/bin/sshd process on affected systems, manipulation occurs.

4 — Symbol Resolution and Function Hooking

Upon loading the backdoored liblzma, the sshd process resolves symbols (functions) within the library. Specific functions related to compression and decompression routines are modified by the backdoor. For instance, it may hook into functions like lzma_decompress or lzma_compress. Altered functions now include additional logic to intercept and manipulate data.

5 — Authentication Flow Interception

During SSH connections, the sshd process manages authentication flows. The backdoor code executes within this context. Modified functions intercept client authentication attempts. Conditions, such as the presence of a predetermined private key, trigger the backdoor.

6 — SSH Access Using Predetermined Private Keys

The attacker possesses a specific private key (e.g., ED488). When connecting to the victim's SSH server, the attacker presents this key. The backdoor allows access, bypassing standard authentication checks. Unauthorized control over the system is achieved using the predetermined private key.

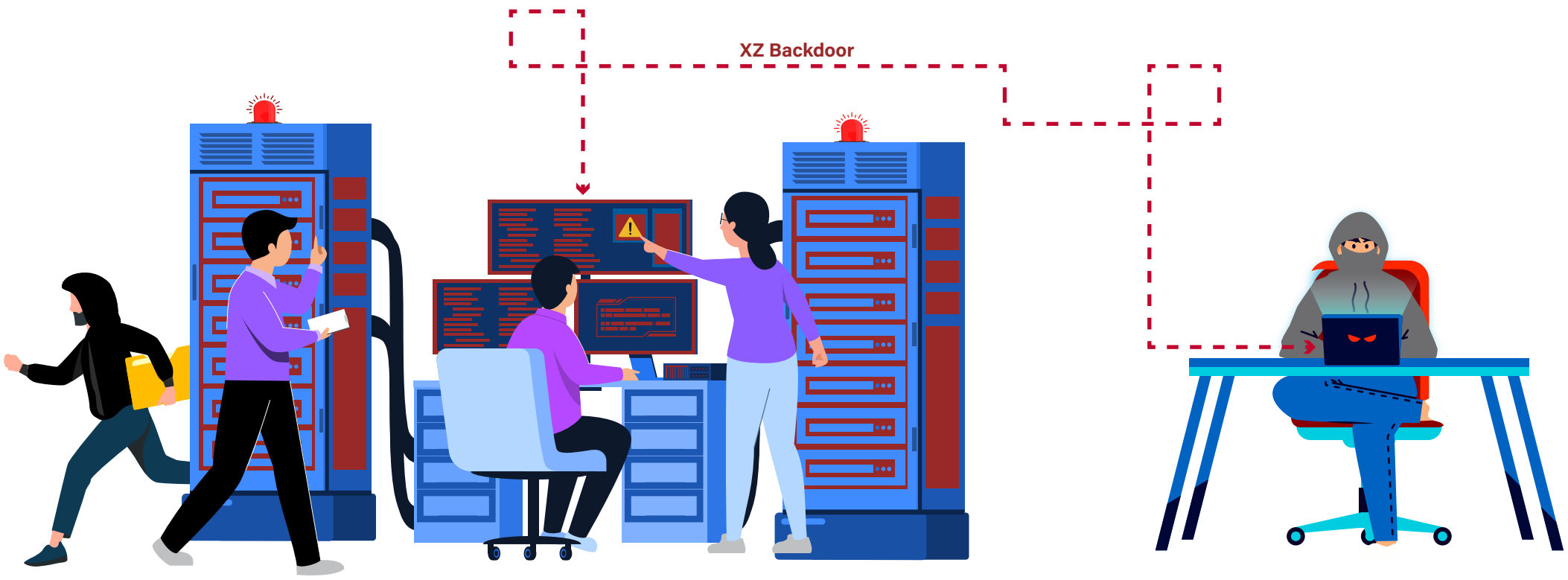
Note: The working of the XZ backdoor, as described here, is based on the current available information. Further investigation and analysis may lead to updates or changes in its functionality.

7. Affected Distribution

Distribution	Affected Distribution	Affected Package
Fedora	Fedora Rawhide and Fedora 40	xz-5.6.0, xz-5.6.1
Debian	Debian Testing, Unstable and experimental	xz-utils 5.5.1alpha-0.1
Alpine	Alpine Edge (active development)	xz 5.6.1-r0, 5.6.1-r1
Kali	Updated Kali between March 26th and March 29th	xz-utils 5.6.0-0.2
Arch Linux	Installation medium 2024.03.01, virtual machine images 20240301.218094 and 20240315.221711, and container images created between and including 2024-02-24 and 2024-03-28	xz 5.6.0, xz-5.6.1
OpenSUSE	OpenSUSE Tumbleweed and MicroOS	xz 5.6.0, xz-5.6.1

8. Impact

This vulnerability has a significant impact, as it allows unauthorized remote SSH access, operates within the same process as the OpenSSH server (SSHD), and alters decryption routines. As a result, specific remote attackers could exploit this vulnerability to inject arbitrary payloads through SSH. These payloads executed before the authentication step, ultimately leading to Remote Code Execution (RCE) and complete hijacking of the victim machine.



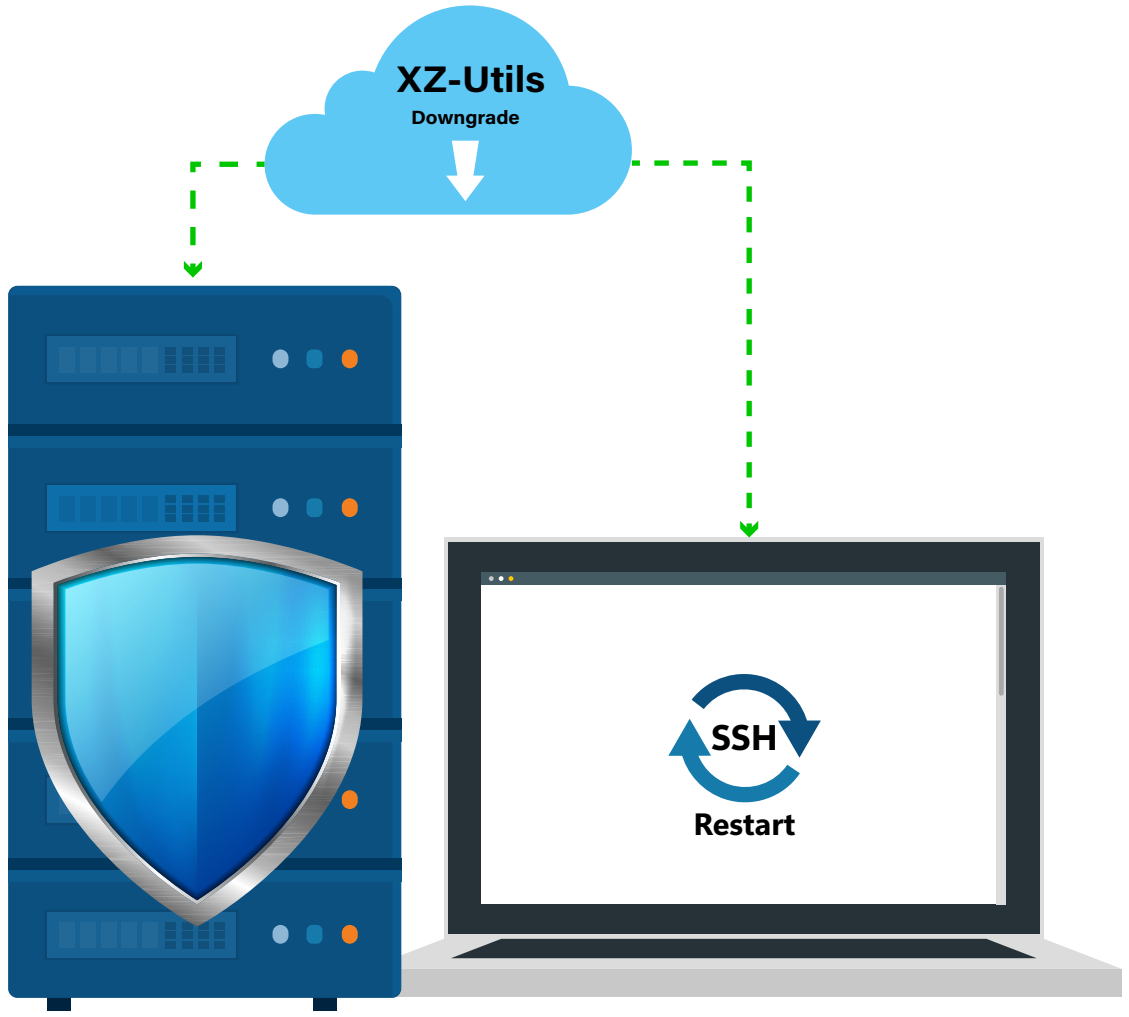
9. Remediation

Downgrade XZ Utils: Take action to revert version of XZ Utils to an earlier iteration, with XZ Utils 5.4.6 identified as the latest unaffected version across most distributions

Restart Services: Following the downgrade of XZ Utils, execute a reboot of your machine or specifically restart the OpenSSH server to eliminate the patched code residing in memory. This can be accomplished by running the command "sudo systemctl restart ssh".

Kill Switch: If upgrading is not a feasible option, implement a workaround by utilizing the backdoor's "kill switch". This involves adding a specific string to the file /etc/environment, effectively disabling the malicious backdoor functionality. This action becomes effective after restarting SSH and Systemd services

Update Installations: Ensure the updating of your installations and packages in accordance with the directions provided by distribution maintainers to mitigate potential vulnerabilities.



7. Additional Resources and References

https://gist.github.com/thesamesam/223949d5a074ebc3dce9ee78baad9e27

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

https://boehs.org/node/everything-i-know-about-the-xz-backdoor

XZ Backdoor Attack CVE-2024-3094: All You Need To Know (jfrog.com)

https://nvd.nist.gov/vuln/detail/CVE-2024-3094

https://github.com/jfrog/cve-2024-3094-tools/tree/main/cve-2024-3094-detector

SECURITYBOAT

Frontline Of Your Business

XZ-UTILS BACKDOOR (CVE-2024-3094)

HANDBOOK

Scan QR Code to Download Handbook

www.securityboat.net