Security Advisory 2024-032

Critical Vulnerability in XZ Utils

April 02, 2024 — v1.1

TLP:CLEAR

History:

- *30/03/2024 — v1.0 – Initial publication*
- *02/04/2024 — v1.1 – Information update*

Summary

[Updated] On March 29, several companies issued a warning regarding a backdoor found in the XZ Utils software. XZ Utils is a data compression software and may be present in Linux distributions. The malicious code may allow a Threat Actor, with the right authentication key, to achieve gated pre-auth RCE on affected systems. [1]

It is recommended downgrading XZ Utils to a not compromised version.

Technical details

[Updated] The issue is tracked as **CVE-2024-3094**, with a CVSS score of 10 out of 10. The malicious code interferes with authentication in `sshd` via `systemd`. Under the right circumstances, this interference allows someone with the right private key to hijack the `sshd` process and from there to execute commands on the targeted system. [1]

Execution chain

[New] The execution chain also consists of multiple stages [7]:

- A malicious script `build-to-host.m4` is run during the library's build process and decodes the "test" file `bad-3-corrupt_lzma2.xz` into a bash script.
- The bash script then performs a more complicated decode process on another "test" file, `good-large_compressed.lzma`, decoding it into another script
- That script then extracts a shared object `liblzma_la-crc64-fast.o`, which is added to the compilation process of `liblzma`

The shared object itself is compiled into `liblzma`, and replaces the regular function name resolution process. The malicious library interferes with the function resolving process, so it could replace the function pointer for the OpenSSH function `RSA_public_decrypt`.

It then points that function to a malicious one of its own which, allegedly, extracts a command from the authenticating client's certificate (after verifying that it is the one of the threat actor) and passes it on to the `system()` function for execution, thereby achieving RCE prior to authentication.

Affected Products

[Updated] XZ Utils has been found compromised starting with version 5.6.0.

Nearly all Linux distributions are using XZ Utils. However, the compromised version was mainly distributed in testing versions of the distributions. The following Linux distributions are known to be affected by the issue:

- Fedora Linux 40 beta [2];
- Fedora Rawhide [2];
- openSUSE Tumbleweed and openSUSE MicroOS [3];
- Debian testing, unstable, and experimental versions [4];
- Kali Linux [5].
- Arch Linux [8]

The following distributions have indicated they are not affected:

- Ubuntu [9]
- Alpine Linux [10]
- Amazon Linux [11]
- Red Hat Enterprise Linux [12]
- Gentoo [13]
- Linux Mint [14]

Please note that this list is not exhaustive as the information about this issue may still be incomplete.

Recommendations

It is strongly advised to immediately stop using affected distribution, or – if possible – downgrade XZ Utils to a version before 5.6.0. It is currently understood that version 5.4.6 should be unaffected. It is advised to prioritise Internet-fronting assets.

References

[1] https://arstechnica.com/security/2024/04/what-we-know-about-the-xz-utils-backdoor-that-almost-infected-the-world/

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

[3] https://news.opensuse.org/2024/03/29/xz-backdoor/

[4] https://lists.debian.org/debian-security-announce/2024/msg00057.html

[5] https://twitter.com/kalilinux/status/1773786266074513523

[6] https://thehackernews.com/2024/03/urgent-secret-backdoor-found-in-xz.html?m=1&s=09

[7] https://www.akamai.com/blog/security-research/critical-linux-backdoor-xz-utils-discovered-what-to-know

[8] https://archlinux.org/news/the-xz-package-has-been-backdoored/

[9] https://ubuntu.com/security/CVE-2024-3094

[10] https://security.alpinelinux.org/vuln/CVE-2024-3094

[11] https://aws.amazon.com/fr/security/security-bulletins/AWS-2024-002/

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

[13] https://security.gentoo.org/glsa/202403-04

[14] https://forums.linuxmint.com/viewtopic.php?t=416756