NVISO CSIRT ADVISORY

DATE (2024-04-02)

SUMMARY

On the 29th of March, 2024, Red Hat Linux disclosed a critical security vulnerability identified as CVE-2024-3094, which has been assigned the highest severity rating of 10 on the CVSS scale. This security flaw stems from a supply chain compromise that affects versions 5.6.0 and 5.6.1 of the XZ Utils software, a program widely used for data compression across numerous Linux distributions. In response to this issue, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) has recommended that users revert to a previous, secure version of XZ Utils, specifically any release prior to version 5.6.0. The latest release that is known as clean is 5.4.6.

XZ Utils was updated to 5.6.0 on the 24th of February 2024 and the update to 5.6.1 was pushed on the 9th of March 2024.

An important remark that we would like to make here is that not all Linux distributions & versions are impacted (mainly the bleeding edge versions). Please refer to the section on “affected products” to verify which ones contain the backdoored version of the software. It is recommended to verify the version of the XZ Utils software using the provided commands.

XZ Utils

XZ Utils is a free software utility for lossless file compression and decompression. It is known for its high compression ratio and efficient performance with a variety of file types. XZ Utils is used in nearly every Linux distribution to compress and decompress data during many different kinds of operations. The tool is used in a wide variety of other software, from hobby and community projects to large commercial products.

As reported by the Red Hat advisory, malicious code was discovered in upstream tarballs of xz, starting with version 5.6.0 and also present in 5.6.1. XZ Utils was updated to 5.6.0 on the 24th of February 2024. The update to 5.6.1 was pushed on the 9th of March 2024.

The build process of the liblzma library has been modified to include intricate obfuscation that culminates in the extraction of a precompiled object file from a camouflaged test file within the source code. This object file is subsequently utilized to alter particular functions in the liblzma code. The outcome is a tampered version of the liblzma library, which, when linked with other software, can intercept and manipulate data interactions involving this library. When the right conditions are present, the code could also allow unauthorized access to any impacted system. So far, it’s reasonably sure that there are the following requirements:

- You need to be running a distro that uses glibc (for IFUNC)
- You need to have versions 5.6.0 or 5.6.1 of xz or liblzma installed (xz-utils provides the library liblzma)

WHY THIS MATTERS

XZ utils is widely distributed on Linux and macOS operating systems. The backdoor which was identified in the XZ package would allow an attacker to connect to an existing SSH service without the need for any authentication. Any internet exposed SSH service could become an easy entry point into the environment.

AFFECTED PRODUCTS

You can verify if a system is vulnerable to the exploit by running the following command:

Distribution	**Command** (Multiple options for Fedora & Alpine)
Red Hat (Fedora)	dnf list installed | grep xz yum list installed | grep xz rpm -qa | grep xz
Debian	dpkg-query -l | grep xz
OpenSUSE	rpm -q liblzma5
Alpine	apk search -v '*xz*' apk search -v | grep xz
Arch	pacman -Q | grep xz

Note: Don't use or rely on the output from a (potentially) compromised tool to check its own version with the command "xz -v".

CPE

Known Affected Software Configurations

- cpe:2.3:a:tukaani:xz:5.6.0:*:*:*:*:*:*:*
- cpe:2.3:a:tukaani:xz:5.6.1:*:*:*:*:*:*:*

Distribution	**Affected version(s)**
Red Hat	Fedora Linux 40 and Fedora Rawhide
Debian	Stable release not affected Testing, unstable and experimental were impacted. Versions 5.5.1alpha-0.1 to 5.6.1-1
Kali	Impacted if updated between March 26-29.
OpenSUSE	Impacted if OpenSUSE Tumbleweed or OpenSUSE Micro OS was updated between March 7-28.
Alpine	5.6 versions prior to 5.6.1-r2
Arch	Installation medium 2024.03.01 Virtual machine images 20240301.218094 and 20240315.221711 Container images created between and including 2024-02-24 and 2024-03-28

HomeBrew doesn't believe their builds were compromised, but as a precautionary measure they are forcing downgrades to 5.4.6.

Amazon Linux customers are not affected as stated by Amazon.

No versions of Red Hat Enterprise Linux (RHEL) are affected.

AVAILABLE WORKAROUNDS

Downgrade to a version lower than 5.6.0. The latest release that is known as clean is 5.4.6.

AVAILABLE PATCHES

No patches are available at time of publication. The XZ GitHub page has been disabled for the time being.

CVE ID, CVSS AND CWE ID

CVE ID	Severity	CVSSv3 Score	CWE ID	CWE Name
CVE-2024-3094	Critical	10.0	CWE-506	Embedded Malicious Code

RECOMMENDED ACTIONS

- Block or restrict SSH access on public facing systems.
- Create an inventory of software that has been updated to XZ 5.6.0 or 5.6.1.
- Downgrade XZ to the latest clean release, version 5.4.6.

CONTACT AND FEEDBACK

Our goal is to provide a fast, brief, and actionable advisory on critical cyber security incidents.

Was this advisory of value to your organization? Was the content clear and concise? Your comments and feedback are very important to us.

Please do not hesitate to reach out to threatintel@nviso.eu

MORE INFORMATION

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

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

CIS advisory: https://www.cisecurity.org/advisory/a-vulnerability-in-xz-utils-could-allow-for-remote-code-execution_2024-033

Red Hat urgent security alert for Fedora Linux 40 and Fedora Rawhide: https://www.redhat.com/en/blog/urgent-security-alert-fedora-41-and-rawhide-users

Red Hat advisory: https://access.redhat.com/security/cve/CVE-2024-3094

Debian security update: https://lists.debian.org/debian-security-announce/2024/msg00057.html

Kali security warning: https://infosec.exchange/@kalilinux/112180505434870941

OpenSUSE advisory: https://news.opensuse.org/2024/03/29/xz-backdoor/

Alpine advisory: https://security.alpinelinux.org/vuln/CVE-2024-3094

Arch advisory: https://archlinux.org/news/the-xz-package-has-been-backdoored/

Microsoft FAQ and guidance for XZ Utils backdoor: https://techcommunity.microsoft.com/t5/microsoft-defender-vulnerability/microsoft-faq-and-guidance-for-xz-utils-backdoor/ba-p/4101961

Palo Alto Threat Brief: https://unit42.paloaltonetworks.com/threat-brief-xz-utils-cve-2024-3094/

XZ Utils git history (GitHub page is disabled at time of writing): https://git.tukaani.org/?p=xz.git;a=summary

Openwall OSS security mailing list post from Andres Freund: https://www.openwall.com/lists/oss-security/2024/03/29/4