April 3, 2024

Overall rating: Critical

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team is aware that Arch Linux have also published security advisories and reversed versions in affected rolling releases.

- *xz libraries - xz-libs-5.6.0-1.fc40.x86_64.rpm*
- *xz-libs-5.6.0-2.fc40.x86_64.rpm.*

Technical Details

As many of you may have already read (one), the upstream release tarballs for xz in version 5.6.0 and 5.6.1 contain malicious code which adds a backdoor.
This vulnerability is tracked in the Arch Linux security tracker (two).
The xz packages prior to version 5.6.1-2 (specifically 5.6.0-1 and 5.6.1-1) contain this backdoor.
The following release artifacts contain the compromised xz:

- 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*

The affected release artifacts have been removed from our mirrors.
We strongly advise against using affected release artifacts and instead downloading what is currently available as latest version!

Upgrading the system

It is strongly advised to do a full system upgrade right away if your system currently has xz version 5.6.0-1 or 5.6.1-1 installed:
pacman -Syu

Exploitability Metrics
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None

This vulnerability is rated as a **CRITICAL** risk. A software update exists to address these risks.

Action Required

- Locate the device or application and investigate.
- Notify business owner(s).
- Perform mitigating actions, as required.

Please notify VRM with any questions or concerns you may have.

References

- CVE-2024-3094
- Arch Linux - News: The xz package has been backdoored