April 2, 2024

Overall rating: Critical

BRITISH COLUMBIA

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team is aware that OpenSUSE security notices to address vulnerabilities in the Linux kernel affecting the following products:

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

Technical Details
Current research indicates that the backdoor is active in the SSH Daemon, allowing malicious actors to access systems where SSH is exposed to the internet.
As of March 29, reverse engineering of the backdoor is still ongoing.
Mitigations
openSUSE Maintainers have rolled back the version of xz on Tumbleweed on March 28 and have released a new Tumbleweed snapshot (20240328 or later) that was built from a safe backup.
The reversed version is versioned 5.6.1.revertto5.4 and can be queried with rpm -q liblzma5.
User recommendation
For our openSUSE Tumbleweed users where SSH is exposed to the internet, we recommend installing fresh, as it's unknown if the backdoor has been exploited.
Due to the sophisticated nature of the backdoor an on-system detection of a breach is likely not possible.
Also rotation of any credentials that could have been fetched from the system is highly recommended.
Otherwise, simply update to openSUSE Tumbleweed 20240328 or later and reboot the system.

- SUSE Security CVE-2024-3094 information page

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
- openSUSE addresses supply chain attack against xz compression library - openSUSE News