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 Debian 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
the upstream source tarballs for xz-utils,
the XZ-format compression utilities, are compromised and inject
malicious code, at build time, into the resulting liblzma5 library.

Right now no Debian stable versions are known to be affected.
Compromised packages were part of the Debian testing, unstable and
experimental distributions, with versions ranging from 5.5.1alpha-0.1
(uploaded on 2024-02-01), up to and including 5.6.1-1. The package has
been reverted to use the upstream 5.4.5 code, which we have versioned
5.6.1+really5.4.5-1.

Users running Debian testing and unstable are urged to update the
xz-utils packages.

For the detailed security status of xz-utils please refer to
its security tracker page at:
https://security-tracker.debian.org/tracker/xz-utils

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
- [SECURITY] [DSA 5649-1] xz-utils security update (debian.org)