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 Fedora Linux 40 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

Red Hat Information Risk and Security and Red Hat Product Security learned that the latest versions of the "xz" tools and libraries **contain malicious code that appears to be intended to allow unauthorized access. Specifically, this code is present in versions 5.6.0 and 5.6.1 of the libraries**. Fedora Linux 40 users may have received version 5.6.0, depending on the timing of system updates. Fedora Rawhide users may have received version 5.6.0 or 5.6.1. This vulnerability was assigned CVE-2024-3094. **PLEASE IMMEDIATELY STOP USAGE OF ANY FEDORA RAWHIDE INSTANCES** for work or personal activity. Fedora Rawhide will be reverted to xz-5.4.x shortly, and once that is done, Fedora Rawhide instances can safely be redeployed. *Note that Fedora Rawhide is the development distribution of Fedora Linux, and serves as the basis for future Fedora Linux builds (in this case, the yet-to-be-released Fedora Linux 41).*

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
- Urgent security alert for Fedora 41 and Fedora Rawhide users (redhat.com)