February 8, 2024

Overall rating: Critical

BRITISH COLUMBIA

This notification is intended as an informational bulletin for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team is aware that Critical vulnerability affecting most Linux distros allows for bootkits

Technical Details

Linux developers are in the process of patching a high-severity vulnerability that, in certain cases, allows the installation of malware that runs at the firmware level, giving infections access to the deepest parts of a device where they're hard to detect or remove.

The vulnerability resides in shim, which in the context of Linux is a small component that runs in the firmware early in the boot process before the operating system has started. More specifically, the shim accompanying virtually all Linux distributions plays a crucial role in secure boot, a protection built into most modern computing devices to ensure every link in the boot process comes from a verified, trusted supplier. Successful exploitation of the vulnerability allows attackers to neutralize this mechanism by executing malicious firmware at the earliest stages of the boot process before the Unified Extensible Firmware Interface firmware has loaded and handed off control to the operating system.

The vulnerability, tracked as CVE-2023-40547, is what's known as a buffer overflow, a coding bug that allows attackers to execute code of their choice. It resides in a part of the shim that processes booting up from a central server on a network using the same HTTP that the the web is based on. Attackers can exploit the code-execution vulnerability in various scenarios, virtually all following some form of successful compromise of either the targeted device or the server or network the device boots from.

.

These vulnerabilities are rated as an overall **Critical** Severity.

Recommended Action

- Investigate how your area of responsibility is affected.
- Notify business owner(s) as required.
- *Ensure mitigation is performed at your next change window.*

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

References

- CVE-2023-40547

- https://arstechnica.com/security/2024/02/critical-vulnerability-affecting-most-linux-distros-allows-for-bootkits/
- https://nvd.nist.gov/vuln/detail/CVE-2023-40547