April 17, 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 Google published a security advisory to address vulnerabilities in the following products:

- Stable channel Chrome for Desktop – versions prior to 124.0.6367.60/.61 (Windows and Mac) and 124.0.6367.60 (Linux)
- Extended Stable channel Chrome for Desktop – versions prior to 14.0.6367.60/.61 (Windows and Mac)

Technical Details
In some code patterns the JIT incorrectly optimized switch statements and generated code with out-of-bounds-reads. This vulnerability affects Firefox < 125 and Firefox ESR < 115.10.

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-2024-3832 CVE-2024-3833 CVE-2024-3914 CVE-2024-3834 CVE-2024-3837 CVE-2024-3838 CVE-2024-3839 CVE-2024-3840 CVE-2024-3841 CVE-2024-3843 CVE-2024-3844 CVE-2024-3845 CVE-2024-3846 CVE-2024-3847
- Google Chrome Security Advisory