May 10, 2024

Overall rating: High

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team has been made aware of a Google Chrome vulnerability actively being exploited in the wild. The vulnerability affects versions prior to 124.0.6367.201/.202 for Mac and Windows and 124.0.6367.201 for Linux.

Technical Details

The vulnerability has been described as a case of use-after-free in the Visuals component. Use-after-free bugs, which arise when a program references a memory location after it has been deallocated, can lead to any number of consequences, ranging from a crash to arbitrary code execution.

Google is aware that an exploit for CVE-2024-4671 exists in the wild.

Exploitability Metrics
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None

This vulnerability is rated as a **HIGH** risk. A software update exists to address this risk.

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-2024-4671
- Stable Channel Update for Desktop
- VRM Vulnerability Reports