

Overall rating: Critical



This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team is aware Google has released a new emergency security update to address the eighth zero-day vulnerability in Chrome browser confirmed to be actively exploited in the wild.

Google is aware that an exploit for CVE-2024-5274 exists in the wild," the company said in the [security advisory](#).

Technical Details

The Stable channel has been updated to 125.0.6422.112/.113 for Windows, Mac and 125.0.6422.112 for Linux which will roll out over the coming days/weeks. A full list of changes in this build is available in the [Log](#).

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-2024-5274](#)
- [Chrome Releases: Stable Channel Update for Desktop \(googleblog.com\)](#)
- [Google fixes eighth actively exploited Chrome zero-day this year \(bleepingcomputer.com\)](#)