May 14, 2024

Overall Rating - High

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

Summary

The Vulnerability and Risk Management (VRM) Team is aware that Google published a security advisory to address a vulnerability in the following products:

- Stable Channel Chrome for Desktop – versions prior to 124.0.6367.207/.208 (Windows and Mac) and 124.0.6367.207 (Linux)
- Extended Stable Channel Chrome for Desktop – versions prior to 124.0.6367.207 (Windows and Mac)

Google has indicated that CVE-2024-4761 has an available exploit.

Technical Details

The Stable channel has been updated to 124.0.6367.207/.208 for Mac and Windows and 124.0.6367.207 for Linux which will roll out over the coming days/weeks. A full list of changes in this build is available in the Log.

Google has released emergency security updates for the Chrome browser to address a high-severity zero-day vulnerability tagged as exploited in attacks.
This fix comes only three days after Google addressed another zero-day vulnerability in Chrome, CVE-2024-4671, caused by a use-after-free weakness in the Visuals component.
The latest bug is tracked as CVE-2024-4761. It is an out-of-bounds write problem impacting Chrome's V8 JavaScript engine, which is responsible for executing JS code in the application. Out-of-bounds write issues occur when a program is allowed to write data outside the specified array or buffer, potentially leading to unauthorized data access, arbitrary code execution, or program crashes.

These vulnerabilities are rated as an overall **High** 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-2024-4761
- Google Chrome Security Advisory

- Google Chrome emergency update fixes 6th zero-day exploited in 2024 (bleepingcomputer.com)