

## 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 the promotion of Chrome 126 to the stable channel for Windows, Mac and Linux. The vulnerability affects versions of Chrome prior to 126.0.6478.54 (Linux) and 126.0.6478.56/57 (Windows, Mac).

### Technical Details

Some of the vulnerabilities addressed in this security update include Type Confusion, Use after free, and Heap buffer overflow vulnerabilities.

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 at [VulnerabilityandRiskManagement@gov.bc.ca](mailto:VulnerabilityandRiskManagement@gov.bc.ca).

### References

- CVE-2024-5830, CVE-2024-5831, CVE-2024-5832, CVE-2024-5833, CVE-2024-5834, CVE-2024-5835, CVE-2024-5836, CVE-2024-5837, CVE-2024-5838, CVE-2024-5839, CVE-2024-5840, CVE-2024-5841, CVE-2024-5842, CVE-2024-5843, CVE-2024-5844, CVE-2024-5845, CVE-2024-5846, CVE-2024-5847
- [Stable Channel Update for Desktop](#)
- [VRM Vulnerability Reports](#)