August 22, 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 Google published a security advisory to address critical vulnerabilities in the following products:

- Stable Channel Chrome for Desktop – versions prior to 128.0.6613.84/.85 (Windows and Mac) and 128.0.6613.84 (Linux)

Google has indicated that CVE-2024-7971 has an available exploit.

Technical Details

Type confusion in V8 in Google Chrome prior to 128.0.6613.84 allowed a remote attacker to exploit heap corruption via a crafted HTML page. (Chromium security severity: High)

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

References

- CVE-2024-7964 CVE-2024-7965 CVE-2024-7966 CVE-2024-7967 CVE-2024-7968 CVE-2024-7969 CVE-2024-7971 CVE-2024-7972 CVE-2024-7973 CVE-2024-7974 CVE-2024-7975 CVE-2024-7976 CVE-2024-7977 CVE-2024-7978 CVE-2024-7979 CVE-2024-7980
- Google Chrome Security Advisory