

Overall Rating: High



This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team has been made aware Palo Alto Networks published security advisories to address vulnerabilities in multiple products. Included were updates for the following:

- Prisma Access Browser – version 128.91.2869.7 and prior
- PAN-OS – versions prior to 11.2.3

Technical Details

Use after free in Passwords in Google Chrome on Android prior to 128.0.6613.84 allowed a remote attacker to potentially 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-2024-8686](#) [CVE-2024-7964](#) [CVE-2024-7965](#) [CVE-2024-7966](#) [CVE-2024-7967](#) [CVE-2024-7968](#) [CVE-2024-7971](#) [CVE-2024-7972](#) [CVE-2024-7973](#) [CVE-2024-7974](#) [CVE-2024-7975](#) [CVE-2024-7976](#) [CVE-2024-7977](#)

[Palo Alto Networks Security Advisories – CVE-2024-8686](#)

[Palo Alto Networks Security Advisories – PAN-SA-2024-0009](#)

[Palo Alto Network Security Advisories](#)