August 16, 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 of Palo Alto Prisma Access Browser vulnerabilities. The vulnerability affects Prisma Access Browser versions prior to 127.100.2858.4.

Technical Details

The impact may allow Type Confusion, Use after free, Out of bounds memory access vulnerabilities and or, Inappropriate implementation and Race Conditions.

Exploitability Metrics
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None

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-2024-6772, CVE-2024-6773, CVE-2024-6774, CVE-2024-6775, CVE-2024-6776, CVE-2024-6777, CVE-2024-6778, CVE-2024-6779, CVE-2024-6988, CVE-2024-6989, CVE-2024-6990, CVE-2024-6991, CVE-2024-6994, CVE-2024-6995, CVE-2024-6996, CVE-2024-6997, CVE-2024-6998, CVE-2024-6999, CVE-2024-7000, CVE-2024-7001, CVE-2024-7003, CVE-2024-7004, CVE-2024-7005, CVE-2024-7256, CVE-2024-7532, CVE-2024-7533, CVE-2024-7534, CVE-2024-7535, CVE-2024-7536, CVE-2024-7550
- PAN-SA-2024-0007 Prisma Access Browser: Monthly Vulnerability Updates
- Stable Channel Update for Desktop July 16, 2024
- Stable Channel Update for Desktop July 23, 2024
- Stable Channel Update for Desktop July 30, 2024
- Stable Channel Update for Desktop August 6, 2024
- VRM Vulnerability Reports