ADV2025_197 Palo Alto Security Advisory (July 15th, 2025)

Palo Alto has published a security advisory highlighting vulnerabilities in the following products on July 9th, 2025. It is recommended that you take the necessary precautions by ensuring your products are always updated.

- Autonomous Digital Experience Manager 5.6.0 macOS – versions prior to 5.6.7
- GlobalProtect App 6.3 macOS – versions prior to 6.3.3-h1 (6.3.3-c650)
- GlobalProtect App 6.2 macOS – versions prior to 6.2.8-h2 (6.2.8-c243)
- GlobalProtect App 6.2 Linux – versions prior to 6.2.8
- GlobalProtect App 6.1 macOS – all versions
- GlobalProtect App 6.1 Linux – all versions
- GlobalProtect App 6.0 macOS – all versions
- GlobalProtect App 6.0 Linux – all versions
- Prisma Access Browser – versions prior to 137.16.6.120

For more information on these updates, you can follow these URLs:

- Palo Alto Networks Security Advisories - PAN-SA-2025-0013 Chromium: Monthly Vulnerability Update (July 2025)
- Palo Alto Networks Security Advisories - CVE-2025-0139 Autonomous Digital Experience Manager: Privilege Escalation (PE) Vulnerability
- Palo Alto Networks Security Advisories - CVE-2025-0140 GlobalProtect App: Non Admin User Can Disable the GlobalProtect App
- Palo Alto Networks Security Advisories - CVE-2025-0141 GlobalProtect App: Privilege Escalation (PE) Vulnerability

The Guyana National CIRT recommends that users and administrators review these updates and apply them where necessary.

References

- Palo Alto Network Security Advisories. (July 9th, 2025). Retrieved from Palo Alto. https://security.paloaltonetworks.com/
- Palo Alto Security Advisory. (July 9th, 2025). Retrieved from Canadian Centre for Cyber Security. www.cyber.gc.ca/en/alerts-advisories/palo-alto-networks-security-advisory-av25-414