ADV2026_73 Palo Alto Networks Security Advisory (February 12th, 2026)

Palo Alto Networks published a security advisory highlighting vulnerabilities in the following products on February 11, 2026. It is recommended that you take the necessary precautions by ensuring your products are always updated.

- PAN-OS 12.1 – versions prior to 12.1.4
- PAN-OS 11.2 – versions prior to 11.2.8
- PAN-OS 11.2 – versions prior to 11.2.10
- PAN-OS 11.1 – versions prior to 11.1.11
- PAN-OS 10.2 – versions prior to 10.2.17
- Prisma Access – versions prior to 11.2.7-h10 on PAN-OS
- Prisma Access – versions prior to 10.2.10-h28 on PAN-OS
- Prisma Browser – versions prior to 144.27.7.133

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

- PAN-SA-2026-0002 Chromium: Monthly Vulnerability Update (February 2026)
- CVE-2026-0228 PAN-OS: Improper Validation of Terminal Server Agent Certificate
- CVE-2026-0229 PAN-OS: Denial of Service in Advanced DNS Security Feature
- Palo Alto Network Security Advisories

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

References

- Palo Alto Networks Security Advisory (February 11th, 2026). Retrieved from Palo Alto Networks. https://security.paloaltonetworks.com/PAN-SA-2026-0002
- Palo Alto Networks Security Advisory. (February 11th, 2026). Retrieved from Canadian Centre for Cyber Security. https://cyber.gc.ca/en/alerts-advisories/palo-alto-networks-security-advisory-av26-118