



CIRT.GY

Guyana National Computer Incident Response Team

ADV2026_221 Palo Alto Security Advisory (April 8th, 2026)

Palo Alto published a security advisory highlighting vulnerabilities in the following products on April 8, 2026. It is recommended that you take the necessary precautions by ensuring your products are always updated.

- Autonomous Digital Experience Manager 5.11.0 – versions prior to 5.11.4
- Cortex XDR Agent 9.0 – versions prior to 9.0.1 without CU-2120 on Windows
- Cortex XDR Agent 8.9 – versions prior to 8.9.1 without CU-2120 on Windows
- Cortex XDR Agent 8.7-CE – versions prior to 8.7.101-CE without CU-2120 on Windows
- Cortex XDR Agent 8.3-CE – all without CI-2120 on Windows
- Cortex XDR Agent 7.9-CE – all without CI-2120 on Windows
- Cortex XSIAM Microsoft Teams Marketplace 1.5.0 – versions prior to 1.5.52
- Cortex XSOAR Microsoft Teams Marketplace 1.5.0 – versions prior to 1.5.52
- Prisma Browser – versions prior to 145.16.12.110

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

- [CVE-2026-0234 Cortex XSOAR: Improper Verification of Cryptographic Signature in Microsoft Teams integration](#)
- [PAN-SA-2026-0004 Chromium: Monthly Vulnerability Update \(April 2026\)](#)
- [CVE-2026-0233 Autonomous Digital Experience Manager: Improper validation of ADEM certificate](#)
- [CVE-2026-0232 Cortex XDR Agent: Local Administrator can disable the agent on Windows](#)

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

References

- Palo Alto Security Advisory (April 8th, 2026). Retrieved from Palo Alto Networks. <https://security.paloaltonetworks.com/>



CIRT.GY

Guyana National Computer Incident Response Team

- Palo Alto Security Advisory (April 8th, 2026). Retrieved from Canadian Centre for Cyber Security. <https://www.cyber.gc.ca/en/alerts-advisories/palo-alto-networks-security-advisory-av26-331>