ADV2026_013 HPE Security Advisory (January 14th, 2026)

HPE published a security advisory addressing vulnerabilities in several products on January 13th, 2026. It is recommended that you take the necessary precautions by ensuring your products are always updated.

- HPE Networking Instant – versions 3.3.1.0 and prior
- HPE Aruba Networking AOS-8 and AOS-10 for Mobility Conductors, Controllers, and Gateways – multiple versions and platforms
- HPE Aruba Networking Virtual Intranet Access (VIA) Client for Linux – versions 4.7.5 and prior

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

- HPESBNW04988 rev.1 - HPE Networking Instant On, Multiple Vulnerabilities
- HPESBNW04987 rev.1 - Multiple Vulnerabilities in HPE Aruba Networking AOS-8 and AOS-10 for Mobility Conductors, Controllers, and Gateways.
- HPESBNW04994 rev.1 - Local Privilege Escalation Vulnerability in HPE Aruba Networking Virtual Intranet Access (VIA) Client for Linux
- HPE Security Bulletin Library

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

References

- HPE Security Advisory. (January 13, 2026). Retrieved from Canadian Centre for Cyber Security. https://www.cyber.gc.ca/en/alerts-advisories/hpe-security-advisory-av26-025
- HPE Security Bulletin Library. (n.d.). Retrieved from HPE. https://support.hpe.com/connect/s/securitybulletinlibrary?language=en_US