ADV2026_124 HPE Security Advisory (March 4th, 2026)

HPE published a security advisory highlighting a vulnerability in the following product on February 27th, 2026. It is recommended that you take the necessary precautions by ensuring your product is always updated.

- HPE AutoPass License Server (APLS) – versions prior to 9.19

For more information on this update, you can follow these URL:

- HPESBGN05003 rev.1 - HPE AutoPass License Server (APLS), Remote Authentication Bypass Vulnerability
- HPE Security Bulletin Library

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

References

- HPESBGN05003 rev.1 - HPE AutoPass License Server (APLS), Remote Authentication Bypass Vulnerability. (February 28, 2026). Retrieved from HPE. https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbgn05003en_us&docLocale=en_US

- HPE Security Bulletin Library. (n.b.). Retrieved from HPE. https://support.hpe.com/connect/s/securitybulletinlibrary?language=en_US

- HPE security advisory. (March 02, 2026). Retrieved from Canadian Centre for Cyber Security. https://www.cyber.gc.ca/en/alerts-advisories/hpe-security-advisory-av26-185