



CIRT.GY

Guyana National Computer Incident Response Team

ADV2025_413 HPE Security Advisory (December 9th, 2025)

HPE published security advisories to address vulnerabilities in the following product on December 4, 2025. It is recommended that you take these necessary precautions by ensuring your products are always updated.

- HP-UX OpenSSL Software – versions prior to A.03.00.17.001

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

- [HPESBUX04977 rev.1 - HP-UX Using OpenSSL, Memory Corruption and Remote Code Execution Vulnerabilities](#)
- [HPE Security Bulletin Library](#)

The Guyana National CIRT recommends that users and administrators review this update and apply it where necessary.

References

- Hewlett Packard Enterprise. (2025, December 4). *HPESBUX04977 Rev.1 - HP-UX using OpenSSL, memory corruption and remote code execution vulnerabilities*. https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbux04977en_us&docLocale=en_US#hpesbux04977-rev-1-hp-ux-using-openssl-memory-corr-0
- Hewlett Packard Enterprise. (n.d.). Security Bulletin Library | HPE Support. [https://support.hpe.com/connect/s/securitybulletinlibrary?language=en_US&archive=false#sort=%40hpescuniversaldate%20descending&layout=table&numberOfResults=25&f:@kmdoclanguagecode=\[cv1871440\]&hpe=1](https://support.hpe.com/connect/s/securitybulletinlibrary?language=en_US&archive=false#sort=%40hpescuniversaldate%20descending&layout=table&numberOfResults=25&f:@kmdoclanguagecode=[cv1871440]&hpe=1)
- HPE Security Advisory. (December 4th, 2025). Retrieved from Canadian Centre for Cyber Security. <https://www.cyber.gc.ca/en/alerts-advisories/hpe-security-advisory-av25-807>