ADV2026_98 HPE Security Advisory (February 19th, 2026)

HPE published a security advisory highlighting vulnerabilities in the following products on February 19, 2026. It is recommended that you take the necessary precautions by ensuring your products are always updated.

- HPE Telco Service Activator – versions prior to 10.5.0
- HPE SimpliVity 380 servers – versions prior to SimpliVity Support Pack (SVTSP) Gen10 and Gen11
- HPE Telco Service Orchestrator – versions prior to v5.5.0

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

- HPESBNW05011 rev.1 - Telco Service Activator, Improper Input Validation
- HPESBHF04967 rev.1 - Certain HPE SimpliVity Servers Using Certain Intel Processor BIOS, INTEL-SA-01234, 2025.3 IPU, UEFI Reference Firmware Advisory., Multiple Vulnerabilities
- HPESBNW04983 rev.1 - HPE Telco Service Orchestrator software, Prototype Pollution Vulnerability
- 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 (February 19th, 2026). Retrieved from HPE. https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw05011en_us&docLocale=en_US#hpesbnw05011-rev-1-telco-service-activator-improper-0
- HPE Security Advisory. (February 19th, 2026). Retrieved from Canadian Centre for Cyber Security. https://cyber.gc.ca/en/alerts-advisories/hpe-security-advisory-av26-150