مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

Security Updates – HPE Products

Tracking #:432317473

Date:10-07-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that recent HPE advisories disclose multiple critical vulnerabilities affecting networking and storage infrastructure. These flaws, if left unpatched, could allow remote attackers to gain unauthorized access or disrupt enterprise operations.

TECHNICAL DETAILS:

HPE has released two security bulletins highlighting vulnerabilities in HPE Networking Instant On Access Points and HPE SANnav Management Portal & Brocade Fabric OS. The issues range from hard-coded credentials to outdated third-party components, with several scoring high on the CVSS scale.

Vulnerability Details (Including but not limited to):

- **CVE-2025-37103**
  - **Description:** Hard-coded login credentials in HPE Networking Instant On Access Points allow remote attackers to bypass authentication.
  - **CVSS Score:** 9.8 (Critical)
  - **Severity:** Critical

- **CVE-2025-4662**
  - **Description:** OpenSSL vulnerability in SANnav 2.4.0a could allow remote code execution.
  - **CVSS Score:** 8.1
  - **Severity:** High

- **CVE-2025-6392**
  - **Description:** Docker-related vulnerability in SANnav 2.4.0a may lead to container escape or privilege escalation.
  - **CVSS Score:** 7.8
  - **Severity:** High

- **CVE-2025-0395**
  - **Description:** Glibc vulnerability in Brocade Fabric OS and SANnav base OS could allow memory corruption.
  - **CVSS Score:** 7.5
  - **Severity:** High

Affected Products

- Brocade 32Gb Fibre Channel SAN Switch for HPE Synergy - 9.1.0 through 9.2.2
- HPE B-series SN3600B Fibre Channel Switch - 9.1.0 through 9.2.2
- HPE B-series SN6600B Fibre Channel Switch - 9.1.0 through 9.2.2
- HPE B-series SN6650B Fibre Channel Switch - 9.1.0 through 9.2.2
- HPE B-series SN6700B Fibre Channel Switch - 9.1.0 through 9.2.2
- HPE B-series SN6750B Fibre Channel Switch - 9.1.0 through 9.2.2

- HPE SN6750B 64Gb 48/128 48-port 64Gb Short Wave SFP56 Port Side Intake Integrated FC Switch - 9.1.0 through 9.2.2
- HPE SN8600B 4-slot SAN Director Switch - 9.1.0 through 9.2.2
- HPE SN8600B 8-slot SAN Director Switch - 9.1.0 through 9.2.2
- HPE SN8700B 4-slot SAN Director Switch - 9.1.0 through 9.2.2
- HPE SN8700B 8-slot SAN Director Switch - 9.1.0 through 9.2.2
- HPE Storage Fibre Channel Switch B-series SN3700B - 9.22
- HPE SANnav Management Software SANnav base OS (OVA deployment) prior to Version 2.4.0a
- HPE Networking Instant On Access Points running software version: 3.2.0.1 and below

Fixed Versions:

- Brocade SANnav version 2.4.0a or later
- Brocade SANnav base OS (OVA deployment) Version 2.4.0a or later
- Brocade Fabric OS 9.2.2a or later
- HPE Networking Instant On software version 3.2.1.0 and above

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to refer to the official HPE security advisory for detailed information on the identified vulnerabilities and to apply the latest security patches as advised to ensure systems are protected.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04894en_us&docLocale=en_US
- https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbst04890en_us&docLocale=en_US