مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates – HPE Products

Tracking #:432317503

Date:18-07-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that HPE released security updates, addressing multiple vulnerabilities in its products. The vulnerabilities could allow attackers to bypass authentication, execute remote code, exfiltrate sensitive data, and cause denial of service in affected HPE software components.

TECHNICAL DETAILS:

The identified vulnerabilities could enable attackers to bypass authentication, execute remote code, exfiltrate sensitive data through SQL injection, and trigger denial of service by exhausting system resources, posing significant risks to system integrity and availability.

Vulnerability Details:

- **CVE-2025-37104**
  - **Base Score**: 7.1
  - **Severity**: High
  - **Affected Versions**: HPE Telco Service Orchestrator - Prior to v5.2.1
  - **Fixed Versions**: HPE Telco Service Orchestrator v5.2.1 or later (minor and maintenance)
  - **Potential Security Impact:** Remote: SQL Injection, Unauthorized Access to Application Database

- **CVE-2022-34917**
  - **Base Score**: 7.5
  - **Severity**: High
  - **Affected Versions**: HPE Telco Service Orchestrator - Prior to v4.2.4
  - **Fixed Versions**: HPE Telco Service Orchestrator v4.2.4 or later.
  - **Potential Security Impact:** Remote: Denial of Service (DoS)

- **CVE-2022-37105 to CVE-2022-37107**
  - **Base Score**: 7.5, 7.3, and 7.3 respectively
  - **Severity**: High
  - **Affected Versions**: HPE AutoPass License Server - prior to 9.18
  - **Fixed Versions**: HPE AutoPass License Server (APLS) 9.18
  - **Potential Security Impact:** Remote: Authentication Bypass, Code Execution, Disclosure of Information

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the latest updates released by HPE.

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=hpesbnw04875en_us&docLocale=en_US
- https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04900en_us&docLocale=en_US
- https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbgn04877en_us&docLocale=en_US