مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Multiple Vulnerabilities in HPE Telco Service Orchestrator

Tracking #:432318881

Date:03-05-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed multiple vulnerabilities in HPE Telco Service Orchestrator software. These vulnerabilities could allow remote attackers to exploit stack overflow conditions, bypass authentication, or potentially achieve full system compromise

TECHNICAL DETAILS:

Vulnerability Details

- **CVE-2026-35554**
  - **Severity:** High | **CVSS:** 8.7
    A high-severity vulnerability in HPE Telco Service Orchestrator could allow remote attackers to bypass authentication and compromise system integrity, potentially resulting in unauthorized access and full compromise of the affected system.
- **CVE-2026-34500**
  - **Severity:** Medium | **CVSS:** 6.5
    A security flaw may allow remote attackers to bypass authentication under specific conditions, which could expose sensitive information or permit unauthorized access.
- **CVE-2026-33532**
  - **Severity:** Medium | **CVSS:** 4.3
    A stack overflow vulnerability may allow attackers with low privileges to impact system availability through crafted network interactions.

Affected Versions

- HPE Telco Service Orchestrator versions prior to v5.6.0

Fixed Versions

- HPE Telco Service Orchestrator v5.6.0 or later

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions 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=hpesbnw05047en_us&docLocale=en_US