مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerability in HPE Telco Service Orchestrator

Tracking #:432318250

Date:14-01-2026

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability in HPE Telco Service Orchestrator software. This vulnerability could allow a remote attacker to exploit a buffer overflow, potentially leading to full system compromise.

TECHNICAL DETAILS:

Vulnerability Details

- **CVE-2025-68615**
- **CVSS v3.1:** 9.8 (Critical)
- The vulnerability exists due to improper handling of input data in HPE Telco Service Orchestrator. A remote attacker can exploit this flaw to trigger a buffer overflow, which may allow arbitrary code execution, data corruption, or system disruption.
- Exploitation of this vulnerability can lead to:
  - Full system compromise
  - Unauthorized access to sensitive data
  - Service disruption

Affected Versions

- HPE Telco Service Orchestrator: All versions prior to v4.2.12

Fixed Version

- HPE Telco Service Orchestrator v4.2.12 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=hpesbnw04993en_us&docLocale=en_US