مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

High-Severity Vulnerability in HPE Telco Service Orchestrator

Tracking #:432318616

Date:17-03-2026

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a high-severity vulnerability in HPE Telco Service Orchestrator (TSO) that could allow remote exploitation of a buffer overflow, potentially leading to service disruption and impacting system availability.

TECHNICAL DETAILS:

A security vulnerability has been identified in HPE Telco Service Orchestrator (TSO) that could allow a remote attacker to exploit a buffer overflow condition. This issue may lead to service disruption and impact system availability.

Vulnerability Details

- **CVE ID:** CVE-2025-52999
- **Severity:** High **CVSS v3.1 Score:** 7.5
- The vulnerability exists in HPE Telco Service Orchestrator and can be exploited remotely without authentication. A successful attack may trigger a buffer overflow condition, potentially causing the application to crash and resulting in a denial-of-service (DoS).

Affected Products

- HPE Telco Service Orchestrator versions prior to 4.2.12

Fixed Versions

- HPE Telco Service Orchestrator v4.2.12 and 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=hpesbnw05029en_us&docLocale=en_US