

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



Security Updates – HPE Telco Service Orchestrator

Tracking #:432317531

Date:25-07-2025

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLIGENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that HPE has released security updates, addressing a vulnerability in its Telco Service Orchestrator. The vulnerability could allow attackers to remotely trigger a Denial of Service (DoS) condition, potentially disrupting system availability.

TECHNICAL DETAILS:

A Remote Denial of Service (DoS) vulnerability has been identified in the HPE Telco Service Orchestrator software. This vulnerability can be remotely exploited to cause repeated IP protocol errors, leading to client starvation and, ultimately, a denial of service.

Vulnerability Details:

- **CVE ID:** CVE-2025-48367
- **V3 Base Score:** 7.5 – High
- **Potential Security Impact:** Remote: Denial of Service (DoS)
- **Affected Products:** HPE Telco Service Orchestrator - Prior to v5.0.2
- **Fixed Versions:** HPE Telco Service Orchestrator v5.0.2 or later.

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=hpesbnw04901en_us&docLocale=en_US