مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

Critical Vulnerability in HPE Telco Service Orchestrator

Tracking #:432317765

Date:01-10-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Hewlett Packard Enterprise (HPE) has released security updates addressing multiple vulnerabilities, including a critical flaw in its Telco Service Orchestrator.

TECHNICAL DETAILS:

Hewlett Packard Enterprise (HPE) has released security updates addressing multiple vulnerabilities, including a critical flaw in its Telco Service Orchestrator. Successful exploitation of these flaws could allow remote attackers to achieve Denial of Service (DoS), SQL Injection, Unauthenticated Information Disclosure, and Buffer Overflow leading to potential code execution or system instability.

Vulnerability Details

Reference	V3 Vector	V3 Base Score
CVE-2025-54419	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H	10.0
CVE-2025-58754	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
CVE-2025-5878	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L	7.3
CVE-2025-8916	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	5.3

Impacted Products:

- HPE Telco Service Orchestrator prior to version 5.3.5

Fixed Version:

- HPE Telco Service Orchestrator v5.3.5 or later

RECOMMENDATIONS:

- Apply Security Updates Immediately-Upgrade HPE Telco Service Orchestrator to fixed version or later, which contains the necessary security fixes.

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.

REFERNCES:

- https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04955en_us&docLocale=en_US