مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerabilities in HPE Telco Service Orchestrator

Tracking #:432317345

Date:04-06-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Hewlett Packard Enterprise (HPE) has released a security bulletin disclosing two vulnerabilities in its Telco Service Orchestrator software.

TECHNICAL DETAILS:

Hewlett Packard Enterprise (HPE) has released a security bulletin disclosing two vulnerabilities in its Telco Service Orchestrator software. These vulnerabilities, tracked as **CVE-2025-31650** and **CVE-2025-31651**, can be exploited **remotely** and may lead to **Access Restriction Bypass** and **Denial of Service (DoS)** attacks.

Vulnerability Details:

1. **CVE-2025-31651**
   - Description: A critical flaw allowing a remote attacker to bypass access restrictions and potentially gain unauthorized access to sensitive systems and data.
   - CVSS v3.1 Base Score: 9.8 (Critical)
   - Impact: Full compromise of confidentiality, integrity, and availability of affected systems.

2. **CVE-2025-31650**
   - Description: A vulnerability that may allow a remote attacker to cause Denial of Service (DoS) without authentication.
   - CVSS v3.1 Base Score: 7.5 (High)
   - Impact: Complete service disruption, potentially affecting telco operations and service availability

Affected Product:

- HPE Telco Service Orchestrator- All versions prior to 5.3.2

Fixed Versions:

- HPE Telco Service Orchestrator v5.3.2 or later.

RECOMMENDATIONS:

- All customers using affected versions of HPE Telco Service Orchestrator must upgrade to fixed version or later as soon as possible.

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=hpesbnw04872en_us&docLocale=en_US