مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerabilities in HPE Telco Unified OSS Console

Tracking #:432317107

Date:23-04-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a Hewlett Packard Enterprise (HPE) has issued a security bulletin detailing several critical vulnerabilities in the HPE Telco Unified OSS Console (UOCAM) software.

TECHNICAL DETAILS:

Hewlett Packard Enterprise (HPE) has issued a security bulletin detailing several critical vulnerabilities in the HPE Telco Unified OSS Console (UOCAM) software prior to version 3.1.15. These flaws encompass both local and remote attack vectors and, if exploited, can lead to remote code execution (RCE), buffer overflows, server-side request forgery (SSRF), and denial of service (DoS) among others.
The vulnerabilities are associated with five CVEs, with CVSS base scores ranging from 4.8 to 9.8, indicating a spectrum from moderate to critical severity.

Vulnerability Details:

CVE	CVSS v3.1	Impact
CVE-2025-24813	9.8 (Critical)	Remote code execution (RCE)
CVE-2025-29774	9.1 (Critical)	Confidentiality/integrity compromise
CVE-2025-29775	9.1 (Critical)	Confidentiality/integrity compromise
CVE-2024-38827	4.8 (Medium)	SSRF, limited data leakage
CVE-2025-27152	5.3 (Medium)	Information disclosure

Fixed Version:

- HPE Telco Unified OSS Console v3.1.15

RECOMMENDATIONS:

- Upgrade HPE Telco Unified OSS Console to fixed version or later.

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=hpesbnw04850en_us&docLocale=en_US