مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

High-Severity Vulnerability in HPE ONMS Adapter

Tracking #:432318298

Date:23-01-2026

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 INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a high-severity vulnerability in the HPE ONMS Adapter component used within HPE Telco IP Mediation that could allow a remote attacker to disrupt services or potentially compromise the system.

TECHNICAL DETAILS:

HPE has identified a remote stack overflow vulnerability in the HPE ONMS Adapter component used within HPE Telco IP Mediation. Successful exploitation could allow a remote attacker to disrupt service or potentially compromise the system.

Vulnerability Details

- **CVE-2024-7254**
- CVSS v3.1 Score: 7.5 (High)
- **Vulnerability Type:** Remote Stack Overflow
- A stack overflow vulnerability exists in the HPE ONMS Adapter component. The issue is triggered when the adapter improperly handles specially crafted network input, leading to a stack overflow condition. An attacker could exploit this vulnerability remotely without authentication, causing the service to crash or enabling further compromise depending on the exploit context.

Impact:

- Remote attackers may cause a stack overflow, leading to denial of service (DoS) or potential system compromise depending on exploitability.

Affected Products

- HPE Telco IP Mediation 8.5.1
  - HPE ONMS Adapter: versions ≤ 4.4.0-0C patch 00001

Fixed Versions

- HPE ONMS Adapter 4.4.0-0C patch 00002 or 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=hpesbnw04990en_us&docLocale=en_US