مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

High-Severity Vulnerability in HP Poly Voice Devices

Tracking #:432318503

Date:03-03-2026

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a high severity vulnerability in HP Poly Voice devices that could allow device impersonation and unauthorized registration with SIP services.

TECHNICAL DETAILS:

A high severity security vulnerability has been identified affecting SIP service providers provisioning Poly Voice devices. The vulnerability may allow device impersonation if an embedded test key and certificate are extracted using specialized reverse engineering techniques. If service providers do not properly validate device certificates during provisioning, unauthorized devices could potentially register with SIP services.

Vulnerability Details

- **CVE ID:** CVE-2026-0754
- **CVSS Score:** 8.2 High
- The vulnerability exists due to an embedded test key and certificate stored within Poly Voice device firmware. If these credentials are extracted, they could be used to impersonate legitimate devices when connecting to SIP service provider environments that do not enforce strict certificate validation. The vulnerability primarily affects provisioning and authentication workflows rather than direct device-to-device communications.
- Successful exploitation could allow attackers to:
  - Impersonate legitimate SIP endpoints
  - Register unauthorized devices to SIP services
  - Access or intercept communication sessions
  - Cause service disruption within voice infrastructures

Affected Products and Fixed Versions

Product Name	Fixed version
VVX	UCS 6.4.8
Edge E	PVOS 8.5.0
Trio 8300	UCS 8.1.7.c

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released by HP.

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.hp.com/us-en/document/ish_14269649-14269682-16/hpsbpy04081