مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical RCE Vulnerability in HP Poly Voice Devices

Tracking #:432319052

Date:02-06-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed HP has disclosed a critical security vulnerability affecting several HP Poly Voice products running on the Linux platform.

TECHNICAL DETAILS:

HP has disclosed a critical security vulnerability affecting several HP Poly Voice products running on the Linux platform. The vulnerability, identified as CVE-2026-0826, may allow an unauthenticated remote attacker to execute arbitrary code on vulnerable devices when Interactive Connectivity Establishment (ICE) is enabled. Successful exploitation could result in complete compromise of affected systems, enabling attackers to gain unauthorized access, execute malicious code, disrupt communications services, and potentially pivot to other network resources.

Vulnerability Details

- CVE ID: CVE-2026-0826
- Vendor: HP Poly
- Product Family: Poly Voice Devices
- Severity: Critical
- CVSS Score: 9.2 (CVSS v4.0)
- HP Security Bulletin: HPSBPY04083 Rev. 1
- Release Date: June 1, 2026
- Potential Impact: Remote Code Execution (RCE)

Affected products

Product	Fixed Firmware Version
VVX Series	UCS 6.4.8 (Pending Release)
Trio 8300	UCS 8.1.7
Trio 8500	UCS 7.2.8
Trio 8800	UCS 7.2.8

RECOMMENDATIONS:

Immediate Actions:

- Apply Security Updates: Upgrade affected devices to the latest available firmware versions.
- Disable ICE Connectivity: Disable Interactive Connectivity Establishment (ICE) on Poly Voice devices if it is not required for business operations.

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/ph-en/document/ish_15052661-15052687-16/hpsbpy04083