مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

High-Severity Vulnerability in HP Poly Video Devices

Tracking #:432318196

Date:31-12-2025

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

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a high-severity vulnerability in HP Poly Video devices, where sensitive data may be written to system log files under specific conditions. The issue is limited in scope and affects administrative operations, potentially exposing sensitive information to users with elevated privileges.

TECHNICAL DETAILS:

A high-severity information disclosure vulnerability has been identified in HP Poly Video devices. In limited scenarios, sensitive data may be written to device log files when administrators perform configuration changes through the Microsoft Teams Admin Center (TAC). Access to these logs is restricted to users with administrative privileges. The issue does not affect configuration changes made via the provisioning server or the device WebUI.

Vulnerability Details

- **CVE-2025-14432**
- **CVSS Score:** 8.1 (High)
- Due to improper handling of configuration data, sensitive information may be logged during TAC-based administrative operations. An attacker with elevated access could potentially retrieve this information from log files, leading to information disclosure.

Affected Products

- Poly G7500
- Poly Studio G62
- Poly Studio X72
- Poly Studio X52
- Poly Studio X32
- Poly Studio X70
- Poly Studio X50
- Poly Studio X30
- Poly Studio E70
- Poly Studio E60
- Poly EagleEye Cube
- Polycom EagleEye IV
- Poly Studio A2
- Poly Studio USB
- TC8
- TC10

Fixed Versions

- **PolyOS 4.6.1-444242** (for Poly Video devices)
- **TCOS 6.6.1-7001859** (for TC8 and TC10)

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the mitigation or workaround provided 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_13612310-13612332-16/hpsbpy04080