مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

High-Severity Vulnerability in HP Poly video conferencing devices

Tracking #:432316487
Date:08-11-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a high-severity vulnerability in HP Poly video conferencing devices that could be exploited to execute malicious code on affected devices.

TECHNICAL DETAILS:

Vulnerability Details:

- **CVE-2024-9579**
- CVSS Score 7.5 High
- A potential remote code execution vulnerability has been identified in certain Poly video conferencing devices. The firmware flaw does not properly sanitize user input, which could potentially allow an attacker to execute arbitrary code on the affected devices
- The exploitation of this vulnerability is dependent on a layered attack and cannot be exploited by itself. This suggests that an attacker would need to chain this vulnerability with other attack vectors to successfully compromise the device.
- If successfully exploited, an attacker could potentially execute arbitrary code on the affected devices, leading to unauthorized access, data theft, or further compromise of the network infrastructure.

Affected products	Fixed Firmware Version
TC8	6.3.2 or higher
TC10	6.3.2 or higher
G7500	4.3.2 or higher
X30	4.3.2 or higher
X50	4.3.2 or higher
X70	4.3.2 or higher
X52	4.3.2 or higher
G62	4.3.2 or higher

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to upgrade the affected versions to the fixed versions at the earliest.

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_11536495-11536533-16/hpsbpy03900