مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Exploited Privilege Escalation Vulnerability in Hikvision IP Cameras

Tracking #:432318524

Date:06-03-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical privilege escalation vulnerability, tracked as CVE-2017-7921, affects multiple Hikvision IP camera models operating with vulnerable firmware versions and is currently being actively exploited by threat actors.

TECHNICAL DETAILS:

A critical privilege escalation vulnerability identified as CVE-2017-7921 affects several Hikvision IP camera models running vulnerable firmware versions. This vulnerability has been included in Known Exploited Vulnerabilities (KEV) catalogs, indicating that it has been actively exploited by threat actors.

Vulnerability Details

- CVE ID: CVE-2017-7921
- Vulnerability Type: Authentication Bypass / Privilege Escalation
- Affected Component: Hikvision IP Camera Web Interface
- Impact: By exploiting this vulnerability, attackers could obtain an unauthorized escalated additional user privilege to acquire or tamper with the device information.

Affected Products:

Product	Vulnerable Firmware Versions	Fixed Version
DS-2CD2xx2F-I Series	V5.2.0 build 140721 – V5.4.0 build 160530	V5.4.5 build 170123+
DS-2CD2xx0F-I Series	V5.2.0 build 140721 – V5.4.0 build 160401	V5.4.5 build 170123+
DS-2CD2xx2FWD Series	V5.3.1 build 150410 – V5.4.4 build 161125	V5.4.5 build 170124+
DS-2CD4x2xFWD Series	V5.2.0 build 140721 – V5.4.0 build 160414	V5.4.5 build 170228+
DS-2CD4xx5 Series	V5.2.0 build 140721 – V5.4.0 build 160421	V5.4.5 build 170302+
DS-2DFx Series	V5.2.0 build 140805 – V5.4.5 build 160928	V5.4.9 build 170123+
DS-2CD63xx Series	V5.0.9 build 140305 – V5.3.5 build 160106	V5.4.5 build 170206+

RECOMMENDATIONS:

Immediate Actions

- Update affected devices to the latest firmware versions provided by the vendor.
- Verify firmware versions across all deployed Hikvision cameras.

Network Security

- Avoid exposing cameras directly to the internet.
- Place surveillance devices in segmented network zones.
- Restrict management access via VPN or secure internal networks.

Access Control

- Change default or weak passwords immediately.
- Enforce strong password policies for administrative accounts.

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://www.hikvision.com/us-en/support/document-center/special-notices/privilege-escalating-vulnerability-in-certain-hikvision-ip-cameras/