# Privilege-Escalating Vulnerability Notice

March 12th, 2017

Dear Valued Customers and Partners:

Hikvision became aware of a privilege-escalating vulnerability that could potentially present a cybersecurity concern under certain, fairly uncommon circumstances. With this announcement, Hikvision would like to notify you that our R&D team has determined that a firmware update will be required to resolve this issue. The issue is resolved once the device is upgraded to the latest firmware.

**What is the privilege-escalating vulnerability?**

When a specific request code is used to access the IP cameras with particular firmware versions directly, it may allow attackers to obtain an unauthorized escalated additional user privilege to acquire or tamper with the device information.

**Which Hikvision products could be affected and how are those cameras accessed?**

This code error only affects the Hikvision IP cameras listed in the attached "Security Notification: Privilege-Escalating Vulnerability in Certain Hikvision IP Cameras."

The overwhelming majority of Hikvision cameras are accessed through a connected NVR, Hikvision iVMS software, or third-party VMS software. As such, it limits the possibility for Hikvision IP cameras to be open to public access, lowering the risk of the cybersecurity exposure. To date, Hikvision is not aware of any reports of malicious activity associated with this vulnerability.

**How is Hikvision resolving this issue?**

In the interest of protecting our customers from any potential cybersecurity threat, Hikvision is taking proactive action to make you aware of this issue, and to inform you of the firmware upgrade, readily available now, that resolves this issue.

**What should users of these particular cameras do?**

Hikvision is advising all users of these cameras to upgrade to the correct firmware version, which fixes this issue. Please refer to the table below.

+1 909-895-0400 Main
+1 866-200-6690 Toll-Free (US & Canada only)

Hikvision USA Inc.
18639 Railroad Street
City of Industry, CA 91748
www.hikvision.com

| Product Name | Affected Versions | Resolved Versions | Where to update firmware |
|---|---|---|---|
| DS-2CD2xx2F-I Series | V5.2.0 build 140721 to V5.4.0 Build 160530 | v5.4.5 Build 170123 and later | **Download Link** |
| DS-2CD2xx0F-I Series | V5.2.0 build 140721 to V5.4.0 Build 160401 | v5.4.5 Build 170123 and later | **Download Link** |
| DS-2CD2xx2FWD Series | V5.3.1 build 150410 to V5.4.4 Build 161125 | v5.4.5 Build 170124 and later | **Download Link** |
| DS-2CD4x2xFWD Series | V5.2.0 build 140721 to V5.4.0 Build 160414 | v5.4.5 Build 170228 and later | **Download Link** |
| DS-2CD4xx5 Series | V5.2.0 build 140721 to V5.4.0 Build 160421 | v5.4.5 Build 170302 and later | **Download Link** |
| DS-2DFx Series | V5.2.0 build 140805 to V5.4.5 Build 160928 | v5.4.9 Build 170123 and later | **Download Link** |
| DS-2CD63xx Series | V5.0.9 build 140305 to V5.3.5 Build 160106 | v 5.4.5 Build 170206 and later | **Download Link** |

Cybersecurity risk is one of the biggest ongoing challenges facing the security industry today. As your trusted partner, we believe it's our responsibility to be vigilant and transparent about cybersecurity threats, to keep you informed, and to employ the industry's best practices. We encourage our partners to take advantage of the many cybersecurity resources Hikvision offers, including the Hikvision Security Center - an industry-leading cybersecurity resource. At the Security Center you can find detailed information about the Hikvision Network and Information Security Lab, third-party and internal testing, and third-party certifications. Additionally, customers can also contact Tech Support or their Hikvision representative anytime with any concerns or questions.

Thank you for your continued support.

Team Hikvision USA Inc. & Hikvision Canada Inc.