Update on Privilege-Escalating Vulnerability Notice

May 4, 2017

Dear Valued Customers and Partners:

Hikvision is honored to work with the U.S. Department of Homeland Security's National Cybersecurity and Communications Integration Center in our ongoing cybersecurity best practice efforts.

We're pleased to announce that Hikvision's successful progress on a privilege-escalating vulnerability has been acknowledged by ICS-CERT (Industrial Control Systems Cyber Emergency Response Team). Specifically, ICS-CERT has recognized that on March 15, 2017 Hikvision released the fixed firmware version 5.4.5 to address the user privilege-escalation vulnerability.

What do customers need to know about the privilege-escalating vulnerability? What steps should customers take to enhance the cybersecurity of Hikvision systems?

- Please review the March 15, 2017 notice, which outlines potential cybersecurity concerns that could arise with specific cameras under certain, fairly uncommon circumstances. To date, Hikvision is not aware of any reports of malicious activity associated with this vulnerability.

- Hikvision always recommends a systematic, multi-step approach to enhance cybersecurity protection. To assist customers and partners, Hikvision offers a number of industry-leading cybersecurity resources. Please visit the Hikvision Security Center for more information.

- The Hikvision Network Security Hardening Guide is a new resource for installers.

- Hikvision also encourages customers to utilize ICS-CERT resources, including ICS-CERT Recommended Practices and ICS Defense in Depth.

Did ICS-CERT recommend further enhancements in future firmware upgrades?

- ICS-CERT identified two areas of potential concern: the configuration file and "gray market" cameras.

Under what circumstances is there a concern with the configuration file? How will Hikvision address this concern?

+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

- The configuration file is encrypted and is therefore not readable, and protects users' credentials. Also, the configuration file can only be exported by the admin account. Hikvision appreciates ICS-CERT's comment, and will enhance the private key decryption storage method in the upcoming firmware release.

What is the concern with "gray market" cameras? Doesn't Hikvision only service cameras that are purchased through authorized channels?

- As always, Hikvision warns potential customers against purchasing from unauthorized distributors. Only authorized Hikvision USA distributors ensure customers receive the benefits of technical support, project registration, and Hikvision USA's full warranty. Click here to see the list of authorized Hikvision distributors.

- Hikvision products purchased from an online source or unauthorized distributor may not be compatible with the North American region's firmware and are considered to be "gray market" product. Updating the firmware from the Hikvision USA site can lead to complications in gray market cameras. Gray market cameras users should upgrade firmware through their original purchasing channel.

- If you have any questions or concerns about the official status of your Hikvision distributor, please contact Hikvision USA Customer Service at csr.usa@hikvision.com.

Hikvision is proud to be at the forefront of the move to improve cybersecurity best practices in our industry. Cybersecurity must be top-of-mind throughout the product lifecycle, from R&D and manufacturing to installation and maintenance. Hikvision's in-house cybersecurity experts are dedicated to constantly assessing and improving our products and our processes, and the Hikvision team provides market-leading cybersecurity education and support to our valued customers. We're also actively engaged with our competitors and partners on collaborative cybersecurity efforts that benefit our entire industry.

Interoperability is key to the success of IP video technology. While it's exciting to watch the ecosystem of video surveillance devices multiply, this also increases our cybersecurity challenges. Establishing interoperability standards for video surveillance should be a top priority and one that everyone in the surveillance industry needs to share.

Team Hikvision USA Inc. & Hikvision Canada Inc.