Hikvision Product Security

Long-term Support Policy

Headquarters
No.555 Qianmo Road, Binjiang District,
Hangzhou 310051, China
T +86-571-8807-5998
overseasbusiness@hikvision.com

Contents

Headquarters
No.555 Qianmo Road, Binjiang District,
Hangzhou 310051, China
T +86-571-8807-5998
overseasbusiness@hikvision.com

1. Brief Introduction

As a global leading IoT solution provider, Hikvision has formed a complete product security management system (refer to *Hikvision Cybersecurity White Paper*, *Hikvision's White Paper on GDPR*). While providing more secure products, it also provides a long-term support policy to quickly respond to cybersecurity issues, so that the customers can use our products at ease.

Our long-term support policy for product security includes the response to security vulnerabilities, the firmware updates, and the provision of firmware with security certification.

The policy is applicable to our DeepinView, Ultra and Smart series network cameras (DS-2CD3XXX, DS-2CD5XXX, DS-2CD7XXX, DS-2DFXXX), DeepinMind NVR, 96000NI-I Series NVR, I Series NVR (DS-76/77/96XXNI-I), and HikCentral VMS products.

Hikvision will provide firmware updates with enhanced security for up to 5 years after discontinuation of their production.

2. Long-term Support Policy

Hikvision long-term support policy provides cybersecurity-related firmware updating services in three stages:

2.1 Intense Firmware Improvement (within 2 years after product launch)

For the first 2 years after product launch, Hikvision updates firmware in an active way, in order to improve the security of products, such as fixing the products' security problems and updating the third-party software library.

The following practices are adopted to enhance the security of our products:

1. Response to security vulnerabilities

Hikvision follows ISO/IEC 30111, ISO/IEC 29147, and other specifications to establish procedures for processing and warning about product security vulnerabilities, obtaining vulnerability information via customers, external CERT, security researchers, and relevant security websites. Once a vulnerability is confirmed, Hikvision will check and fix it. The fixed firmware will be immediately sent to customers, and Hikvision will disclose the security vulnerability and

release the fixed firmware on its website.

(https://www.hikvision.com/en/Support/Cybersecurity-Center/Security-Advisory)

2. Constant improvement of product security

As the attack techniques of the hackers develop, the security of products also needs constant enhancement. Hikvision complies with the best security practices in the industry to publish the updated firmware for products on a regular basis (see the website below). The security improvements are introduced in the product security instructions.
(https://www.hikvision.com/en/Support/Cybersecurity-Center/Best-Practices)

3. Firmware with security certification

To meet the growing expectation of product security, Hikvision has already had some products certified by CC (Common Criteria Certification), FIPS 140-2 Certification and other international product security certifications. We provide firmware with security certification to these products, so that users can use our products without worrying about the security.

And we have concrete and continuous plans to get more products certified in the years to come.

2.2 Dynamic Firmware Improvement (2 years after launch - discontinuation)

Hikvision will continue to update firmware to address confirmed and potential security risks and ensure secure operations of products 2 years after the product release until the discontinuation of production.

Any security-related firmware update will be announced to customers through the official website as quickly as possible. The announcement will also include the security risks and related operations involved in the firmware update. The firmware itself will also be released on the official website for timely access by customers.

2.3 Constant Updating of Security Firmware (within 5 years after the discontinuation)

If within 5 years after the announcement of production discontinuation, a product shows severe security vulnerability pursuant to the Common Vulnerability Scoring System 3.0 (CVSS 3.0), Hikvision will continue to provide necessary updated firmware.