Hanwha Vision

6, Pangyo-ro 319beon-gil, Bundang-gu, Seongnam-si, Gyeonggi-do, 13488, Korea
TEL 82.70.7147.7000 FAX 82.31.8018.3702 www.HanwhaVision.com

2024 Hanwha Vision S-Cert Team

March 2024

# NVR, DVR Vulnerability Report (CVE-2023-6095, 6096)

## ■ OVERVIEW

- Vladimir Kononovich who is one of our customers at Ukraine discovered two vulnerabilities in the Hanwha HRX-1620 DVR and reported it to the Hanwha S-CERT on September 15th, 2023.
- These vulnerabilities are regarding Remote Code Execution without authentication using stack overflow and implementing with inappropriate encryption logic.

| CVE | Description |
|---|---|
| CVE-2023-6095 | Remote Code Execution without authentication using stack overflow |
| CVE-2023-6096 | Implementing with inappropriate encryption logic |

## ■ AFFECTED PRODUCTS AND FIRMWARE

- These vulnerabilities **CVE-2023-6095,6096** affect specific NVR/DVR models.
- Refer to the below table for the affected model, affected firmware version, and corrected firmware version.

| Model | Affected Firmware Version | Corrected Firmware Version |
|---|---|---|
| XRN-2010 | 2.46 and prior versions | 2.70 and later versions |
| XRN-2011 | 2.46 and prior versions | 2.70 and later versions |
| XRN-3010 | 2.46 and prior versions | 2.70 and later versions |
| XRN-2010A | 2.46 and prior versions | 2.70 and later versions |
| XRN-2011A | 2.46 and prior versions | 2.70 and later versions |
| XRN-3010A | 2.46 and prior versions | 2.70 and later versions |
| ARN-3250 | 2.46 and prior versions | 2.70 and later versions |
| XRN-810S | 2.46 and prior versions | 2.70 and later versions |
| XRN-410S | 2.46 and prior versions | 2.70 and later versions |
| QRN-810 | 2.46 and prior versions | 2.70 and later versions |
| QRN-410 | 2.46 and prior versions | 2.70 and later versions |

Hanwha Vision
6, Pangyo-ro 319beon-gil, Bundang-gu, Seongnam-si, Gyeonggi-do, 13488, Korea
TEL 82.70.7147.7000 FAX 82.31.8018.3702 www.HanwhaVision.com

| | | |
|---|---|---|
| HRX-1621 | 3.05.62 and prior versions | 3.05.72 and later versions |
| HRX-1620 | 3.05.62 and prior versions | 3.05.72 and later versions |
| HRX-821 | 3.05.62 and prior versions | 3.05.72 and later versions |
| HRX-820 | 3.05.62 and prior versions | 3.05.72 and later versions |
| HRX-421 | 3.05.62 and prior versions | 3.05.72 and later versions |
| HRX-420 | 3.05.62 and prior versions | 3.05.72 and later versions |
| XRN-420S | 5.01.52 and prior versions | 5.01.62 and later versions |
| QRN-430S | 5.01.52 and prior versions | 5.01.62 and later versions |

## RISK ANALYSIS

| CVE | Review Opinion | Severity |
|---|---|---|
| CVE-2023-6095 | An attacker could inject arbitrary attack code by manipulating HTTP headers. However, in order to succeed in the attack, the base address of the stack memory must be obtained. The default address depends on firmware version, configuration option information, and the attack is unlikely to succeed. Nevertheless, we believe that this vulnerability has a significant impact on the product because it allows arbitrary attacks without authentication. | High |
| CVE-2023-6096 | By dismantling the firmware, an attacker can analyze internal information, as well as configure the manipulated firmware to update the product. If the attacker has the ability to log into the product, they can take control of it. | Middle |

## ■ Solution and Required Action

- As some models do not fall under Hanwha's long-term firmware support policy when they were discontinued, it is not mandatory to distribute firmware that corrects security vulnerabilities. However, since Hanwha takes cybersecurity matters seriously, we distribute corrected firmware out of consideration for customers in this case.
- Please update the affected models with the latest firmware as soon as possible. It is recommended to use the Wisenet Device Manager tool to download & update device firmware. Firmware can also be downloaded from Hanwha Vision websites.

Hanwha Vision

6, Pangyo-ro 319beon-gil, Bundang-gu, Seongnam-si, Gyeonggi-do, 13488, Korea
TEL 82.70.7147.7000 FAX 82.31.8018.3702 www.HanwhaVision.com

- If you have any questions, please feel free to reach out the Hanwha S-CERT team at secure.cctv@hanwha.com or your local Technical Support Team.