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

Hanwha Vision S-Cert Team

December 2024

NVR Vulnerability Report (CVE-2024-41882 ~ 41887)

■ OVERVIEW

- Team ENVY, a Security Research Team discovered vulnerability in the Hanwha XRN-420S and reported it to the Hanwha S-CERT on July 15th, 2024. These vulnerabilities compromise the availability of the NVR and are related to the hardcoding of sensitive information. We have analyzed the impact of this vulnerability and are working to quickly provide a patch firmware.

CVE	vulnerability
CVE-2024-41887	Arbitrary File Overwrite
CVE-2024-41886	Improper Input Validation
CVE-2024-41885	Hardcoding sensitive information
CVE-2024-41884	Null Pointer Dereference #1
CVE-2024-41883	Null Pointer Dereference #2
CVE-2024-41882	Stack based buffer overflow

■ AFFECTED PRODUCTS AND FIRMWARE

- These vulnerabilities CVE-2024-41882~41887 affect specific NVR 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-420S	5.01.62 and prior versions	5.01.72 and later versions
QRN-430S	5.01.62 and prior versions	5.01.72 and later versions
HRX-1632	4.52.62 and prior versions	4.52.72 and later versions
HRX-835	4.52.62 and prior versions	4.52.72 and later versions
HRX-435	5.31.72 and prior versions	5.31.82 and later versions
HRX-434	5.31.72 and prior versions	5.31.82 and later versions
HRX-1635	5.31.72 and prior versions	5.31.82 and later versions
HRX-1634	5.31.72 and prior versions	5.31.82 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-835A	5.31.72 and prior versions	5.31.82 and later versions
HRX-435L	5.31.72 and prior versions	5.31.82 and later versions
XRN-426S	5.33.12 and prior versions	5.33.22 and later versions
PRN-6410B4	5.34.12 and prior versions	5.34.22 and later versions
PRN-3210B4	5.34.12 and prior versions	5.34.22 and later versions
PRN-3210B2	5.34.12 and prior versions	5.34.22 and later versions
PRN-1610B2	5.34.12 and prior versions	5.34.22 and later versions
PRN-6405DB4	5.34.12 and prior versions	5.34.22 and later versions
PRN-6405B4	5.34.12 and prior versions	5.34.22 and later versions
PRN-3205B4	5.34.12 and prior versions	5.34.22 and later versions
PRN-3205B2	5.34.12 and prior versions	5.34.22 and later versions
PRN-1605B2	5.34.12 and prior versions	5.34.22 and later versions
PRN-6400DB4	5.34.12 and prior versions	5.34.22 and later versions
PRN-6400B4	5.34.12 and prior versions	5.34.22 and later versions
PRN-3200B4	5.34.12 and prior versions	5.34.22 and later versions
PRN-3200B2	5.34.12 and prior versions	5.34.22 and later versions
PRN-1600B2	5.34.12 and prior versions	5.34.22 and later versions
XRN-6410DB4	5.34.12 and prior versions	5.34.22 and later versions
XRN-6410B4	5.34.12 and prior versions	5.34.22 and later versions
XRN-3210B4	5.34.12 and prior versions	5.34.22 and later versions
XRN-6410RB2	5.34.12 and prior versions	5.34.22 and later versions
XRN-6410B2	5.34.12 and prior versions	5.34.22 and later versions
XRN-3210RB2	5.34.12 and prior versions	5.34.22 and later versions
XRN-3210B2	5.34.12 and prior versions	5.34.22 and later versions
XRN-1620B2	5.34.12 and prior versions	5.34.22 and later versions
XRN-1620SB1	5.34.12 and prior versions	5.34.22 and later versions
XRN-820S	5.34.12 and prior versions	5.34.22 and later versions
ARN-1610S	5.31.42 and prior versions	5.31.52 and later versions
ARN-810S	5.31.42 and prior versions	5.31.52 and later versions
ARN-410S	5.31.42 and prior versions	5.31.52 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

XRN-815S	5.06.52 and prior versions	5.06.62 and later versions
QRN-1630S	5.06.52 and prior versions	5.06.62 and later versions
QRN-830S	5.06.52 and prior versions	5.06.62 and later versions
XRN-425S	5.31.32 and prior versions	5.31.42 and later versions
SPD-152	5.10.32 and prior versions	5.10.42 and later versions
ARD-1610	5.31.32 and prior versions	5.31.42 and later versions
ARD-810	5.31.32 and prior versions	5.31.42 and later versions
ARD-410	5.31.32 and prior versions	5.31.42 and later versions
HRX-1635/TE	5.31.72 and prior versions	5.31.82 and later versions
HRX-835/TE	5.31.72 and prior versions	5.31.82 and later versions
HRX-435FN/TE	5.31.72 and prior versions	5.31.82 and later versions
XRN-6410DR/TE	5.34.12 and prior versions	5.34.22 and later versions
XRN-6410R/TE	5.34.12 and prior versions	5.34.22 and later versions
XRN-3210R/TE	5.34.12 and prior versions	5.34.22 and later versions
XRN-1620S/TE	5.34.12 and prior versions	5.34.22 and later versions
XRN-820S/TE	5.34.12 and prior versions	5.34.22 and later versions
XRN-6410B4/TU	5.34.12 and prior versions	5.34.22 and later versions
HRX-1635/TU	5.12.22 and prior versions	5.12.32 and later versions
XRN-425SFN/TE	5.31.32 and prior versions	5.31.42 and later versions

RISK ANALYSIS

CVE	Review Opinion	Severity
CVE-2024-41887	An attacker can exploit the log generation feature in the NVR to generate logs in a directory one level higher than the specified log generation directory. However, the attacker needs to have ADMIN authentication privileges on the NVR, and cannot change the path to any other directory. Because the exploit is so limited, it is not attractive to attackers.	low
CVE-2024-41886	An attacker can intentionally cause the NVR to reboot by entering malformed data into certain URL input parameters. This has the limitation that the attacker needs access to the NVR's web admin	medium

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

	page. However, this attack can be carried out continuously, so it is recommended to update to patched firmware.	
CVE-2024-41885	The seed string for the encrypt key was hardcoding. This issue can be escalated to an issue where the NVR firmware decryption key can be reproduced if the seed string is leaked. but, reverse-engineering the encrypted NVR firmware to verify the seed string is a difficult task. Nevertheless, we recommend updating to patched firmware.	low
CVE-2024-41884	an attacker does not enter a specific URL parameter value, a NULL pointer reference occurs and the NVR is rebooted. This attack is limited in that it requires privileges to be successful, but it is recommended to update to the patched firmware as it can be continuously attacked.	medium
CVE-2024-41883	an attacker enters a specific value for a specific URL parameter value, a NULL pointer reference occurs and the NVR is rebooted. This attack is limited in that it requires privileges to be successful, but it is recommended to update to the patched firmware as it can be continuously attacked.	medium
CVE-2024-41882	An attacker can cause a stack overflow by entering large data into URL parameters, which will result in NVR reboot. This attack is limited in that it requires privileges to be successful, but it is recommended to update to the patched firmware as it can be continuously attacked.	medium

■ Solution and Required Action

- 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.
- 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.