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

Jun 2024

Camera Vulnerability Report (CVE-2023-5037, 5038)

■ OVERVIEW

- Badmonkey, a security researcher, discovered two vulnerabilities in Camera and reported them to Hanwha Vision S-CERT on July 12, 2023.
- These two vulnerabilities are an authenticated command injection vulnerability that executes OS commands and unauthenticated deny of service vulnerability.

CVE	Description
CVE-2023-5037	authenticated command injection using http parameter
CVE-2023-5038	unauthenticated deny of service using http parameter

■ RISK ANALYSIS

CVE	Review Opinion	Severity
CVE-2023-5037	An attacker can inject arbitrary OS commands by manipulating HTTP parameters. The execution of arbitrary OS commands can be used to inject malware or configure a backdoor. However, the attack requires credentials from the camera web admin page to succeed. This means that the vulnerability is only triggered if the attacker is authorized to log into the product.	Middle
CVE-2023-5038	An error was found in the camera's web service that could cause exception handling logic to be executed in an improper manner. An attacker could execute a crafted URL to trigger an unauthenticated DoS attack. In this case, no one can access the camera's web management page, and the device must be manually restarted or powered back on. This vulnerability is considered to have a significant impact on the product because it allows attacks without authentication.	High

■ AFFECTED PRODUCTS AND FIRMWARE

- These vulnerabilities CVE-2023-5037, 5038 affect specific Camera models.
- Refer to the below table for the affected model, affected firmware version, and corrected firmware version.

Model	Affected Firmware Version	Corrected Firmware Version
ANO-L6012R	Prior to version 1.41.16	Version 1.41.16 and later
ANO-L6022R	Prior to version 1.41.16	Version 1.41.16 and later
ANV-L6012R	Prior to version 1.41.16	Version 1.41.16 and later
ANO-L6082R	Prior to version 1.41.16	Version 1.41.16 and later
ANE-L6012R	Prior to version 1.41.16	Version 1.41.16 and later
ANV-L6082R	Prior to version 1.41.16	Version 1.41.16 and later
ANO-L7082R	Prior to version 1.41.16	Version 1.41.16 and later
ANE-L7012R	Prior to version 1.41.16	Version 1.41.16 and later
ANV-L7082R	Prior to version 1.41.16	Version 1.41.16 and later
ANO-L7012R	Prior to version 1.41.16	Version 1.41.16 and later
ANO-L7022R	Prior to version 1.41.16	Version 1.41.16 and later
ANV-L7012R	Prior to version 1.41.16	Version 1.41.16 and later
PNM-C9022RV	Prior to version 2.22.02	Version 2.22.02 and later
PNM-9000QB	Prior to version 2.22.01	Version 2.22.01 and later
PNM-7002VD	Prior to version 2.22.02	Version 2.22.02 and later
PNM-8082VT	Prior to version 2.22.00	Version 2.22.00 and later
PNM-9002VQ	Prior to version 2.22.02	Version 2.22.02 and later
PNM-9022V	Prior to version 2.22.00	Version 2.22.00 and later
PNM-9031RV	Prior to version 2.22.01	Version 2.22.01 and later
PNM-9084QZ	Prior to version 2.22.02	Version 2.22.02 and later
PNM-9084RQZ	Prior to version 2.22.02	Version 2.22.02 and later
PNM-9085RQZ	Prior to version 2.22.02	Version 2.22.02 and later
PNM-9084QZ1	Prior to version 2.22.02	Version 2.22.02 and later
PNM-9084RQZ1	Prior to version 2.22.02	Version 2.22.02 and later
PNM-9085RQZ1	Prior to version 2.22.02	Version 2.22.02 and later
PNM-9322VQP	Prior to version 2.22.02	Version 2.22.02 and later
PNM-7082RVD	Prior to version 2.22.02	Version 2.22.02 and later
PNM-12082RVD	Prior to version 2.22.02	Version 2.22.02 and later
LNO-6072R	Prior to version 1.41.13	Version 1.41.13 and later
LND-6012R	Prior to version 1.41.13	Version 1.41.13 and later
LNO-6032R	Prior to version 1.41.13	Version 1.41.13 and later
LNV-6032R	Prior to version 1.41.13	Version 1.41.13 and later

LND-6022R	Prior to version 1.41.13	Version 1.41.13 and later
LND-6072R	Prior to version 1.41.13	Version 1.41.13 and later
LNO-6022R	Prior to version 1.41.13	Version 1.41.13 and later
LNV-6012R	Prior to version 1.41.13	Version 1.41.13 and later
LNV-6072R	Prior to version 1.41.13	Version 1.41.13 and later
LND-6032R	Prior to version 1.41.13	Version 1.41.13 and later
LNV-6022R	Prior to version 1.41.13	Version 1.41.13 and later
LNO-6012R	Prior to version 1.41.13	Version 1.41.13 and later
QND-6011	Prior to version 1.41.16	Version 1.41.16 and later
QND-6012R	Prior to version 1.41.16	Version 1.41.16 and later
QND-6021	Prior to version 1.41.16	Version 1.41.16 and later
QND-6022R	Prior to version 1.41.16	Version 1.41.16 and later
QND-6032R	Prior to version 1.41.16	Version 1.41.16 and later
QND-6072R	Prior to version 1.41.16	Version 1.41.16 and later
QND-6073R	Prior to version 1.41.16	Version 1.41.16 and later
QND-6082R	Prior to version 1.41.16	Version 1.41.16 and later
QND-6083R	Prior to version 1.41.16	Version 1.41.16 and later
QNO-6012R	Prior to version 1.41.16	Version 1.41.16 and later
QNO-6022R	Prior to version 1.41.16	Version 1.41.16 and later
QNO-6032R	Prior to version 1.41.16	Version 1.41.16 and later
QNO-6072R	Prior to version 1.41.16	Version 1.41.16 and later
QNO-6073R	Prior to version 1.41.16	Version 1.41.16 and later
QNO-6082R	Prior to version 1.41.16	Version 1.41.16 and later
QNO-6083R	Prior to version 1.41.16	Version 1.41.16 and later
QNV-6012R	Prior to version 1.41.16	Version 1.41.16 and later
QNV-6022R	Prior to version 1.41.16	Version 1.41.16 and later
QNV-6032R	Prior to version 1.41.16	Version 1.41.16 and later
QNV-6072R	Prior to version 1.41.16	Version 1.41.16 and later
QNV-6073R	Prior to version 1.41.16	Version 1.41.16 and later
QNV-6082R	Prior to version 1.41.16	Version 1.41.16 and later
QNV-6083R	Prior to version 1.41.16	Version 1.41.16 and later
QND-6012R1	Prior to version 1.41.16	Version 1.41.16 and later
QND-6022R1	Prior to version 1.41.16	Version 1.41.16 and later
QND-6032R1	Prior to version 1.41.16	Version 1.41.16 and later
QND-6072R1	Prior to version 1.41.16	Version 1.41.16 and later
QND-6082R1	Prior to version 1.41.16	Version 1.41.16 and later
QNV-6012R1	Prior to version 1.41.16	Version 1.41.16 and later
QNV-6022R1	Prior to version 1.41.16	Version 1.41.16 and later
QNV-6032R1	Prior to version 1.41.16	Version 1.41.16 and later

QNV-6072R1	Prior to version 1.41.16	Version 1.41.16 and later
QNV-6082R1	Prior to version 1.41.16	Version 1.41.16 and later
QNO-6012R1	Prior to version 1.41.16	Version 1.41.16 and later
QNO-6022R1	Prior to version 1.41.16	Version 1.41.16 and later
QNO-6032R1	Prior to version 1.41.16	Version 1.41.16 and later
QNO-6072R1	Prior to version 1.41.16	Version 1.41.16 and later
QNO-6082R1	Prior to version 1.41.16	Version 1.41.16 and later
QND-7082R	Prior to version 1.41.16	Version 1.41.16 and later
QNV-7082R	Prior to version 1.41.16	Version 1.41.16 and later
QNO-7082R	Prior to version 1.41.16	Version 1.41.16 and later
QND-7012R	Prior to version 1.41.16	Version 1.41.16 and later
QND-7022R	Prior to version 1.41.16	Version 1.41.16 and later
QND-7032R	Prior to version 1.41.16	Version 1.41.16 and later
QNO-7012R	Prior to version 1.41.16	Version 1.41.16 and later
QNO-7022R	Prior to version 1.41.16	Version 1.41.16 and later
QNO-7032R	Prior to version 1.41.16	Version 1.41.16 and later
QNV-7012R	Prior to version 1.41.16	Version 1.41.16 and later
QNV-7022R	Prior to version 1.41.16	Version 1.41.16 and later
QNV-7032R	Prior to version 1.41.16	Version 1.41.16 and later
QNV-6014R	Prior to version 1.41.16	Version 1.41.16 and later
QNV-6084R	Prior to version 1.41.16	Version 1.41.16 and later
QNO-6014R	Prior to version 1.41.16	Version 1.41.16 and later
QNO-6084R	Prior to version 1.41.16	Version 1.41.16 and later
QNV-6024RM	Prior to version 1.41.16	Version 1.41.16 and later
QNV-6023R	Prior to version 1.41.16	Version 1.41.16 and later
ANV-L6023R	Prior to version 1.41.16	Version 1.41.16 and later
QNB-8002	Prior to version 1.41.17	Version 1.41.17 and later
QND-8010R	Prior to version 1.42.01	Version 1.42.01 and later
QND-8011	Prior to version 1.42.01	Version 1.42.01 and later
QND-8020R	Prior to version 1.42.01	Version 1.42.01 and later
QND-8021	Prior to version 1.42.01	Version 1.42.01 and later
QND-8030R	Prior to version 1.42.01	Version 1.42.01 and later
QND-8080R	Prior to version 1.42.01	Version 1.42.01 and later
QNE-8011R	Prior to version 1.42.01	Version 1.42.01 and later
QNE-8021R	Prior to version 1.42.01	Version 1.42.01 and later
QNO-8010R	Prior to version 1.42.01	Version 1.42.01 and later
QNO-8020R	Prior to version 1.42.01	Version 1.42.01 and later
QNO-8030R	Prior to version 1.42.01	Version 1.42.01 and later
QNO-8080R	Prior to version 1.42.01	Version 1.42.01 and later

QNV-8010R	Prior to version 1.42.01	Version 1.42.01 and later
QNV-8020R	Prior to version 1.42.01	Version 1.42.01 and later
QNV-8030R	Prior to version 1.42.01	Version 1.42.01 and later
QNV-8080R	Prior to version 1.42.01	Version 1.42.01 and later
XNV-9083RZ	Prior to version 2.23.00	Version 2.23.00 and later
XNV-8083RZ	Prior to version 2.23.00	Version 2.23.00 and later
XNV-8083Z	Prior to version 2.23.00	Version 2.23.00 and later
XNV-6083RZ	Prior to version 2.23.00	Version 2.23.00 and later
XNV-6083Z	Prior to version 2.23.00	Version 2.23.00 and later
XNB-6002	Prior to version 2.23.00	Version 2.23.00 and later
XND-6083RV	Prior to version 2.23.00	Version 2.23.00 and later
XNV-6083R	Prior to version 2.23.00	Version 2.23.00 and later
XNO-6083R	Prior to version 2.23.00	Version 2.23.00 and later
XNB-6003	Prior to version 2.23.00	Version 2.23.00 and later
XNV-9083R	Prior to version 2.23.00	Version 2.23.00 and later
XNV-8093R	Prior to version 2.23.00	Version 2.23.00 and later
XNV-8083R	Prior to version 2.23.00	Version 2.23.00 and later
XND-9083RV	Prior to version 2.23.00	Version 2.23.00 and later
XND-8093RV	Prior to version 2.23.00	Version 2.23.00 and later
XND-8083RV	Prior to version 2.23.00	Version 2.23.00 and later
XNO-9083R	Prior to version 2.23.00	Version 2.23.00 and later
XNO-8083R	Prior to version 2.23.00	Version 2.23.00 and later
XNB-9003	Prior to version 2.23.00	Version 2.23.00 and later
XNB-8003	Prior to version 2.23.00	Version 2.23.00 and later
XND-C6083RV	Prior to version 2.23.00	Version 2.23.00 and later
XND-C7083RV	Prior to version 2.23.00	Version 2.23.00 and later
XNV-C6083R	Prior to version 2.23.00	Version 2.23.00 and later
XNV-C7083R	Prior to version 2.23.00	Version 2.23.00 and later
XNO-C6083R	Prior to version 2.23.00	Version 2.23.00 and later
XNO-C7083R	Prior to version 2.23.00	Version 2.23.00 and later
XNV-C6083	Prior to version 2.23.00	Version 2.23.00 and later
XND-C8083RV	Prior to version 2.23.00	Version 2.23.00 and later
XND-C9083RV	Prior to version 2.23.00	Version 2.23.00 and later
XNV-C8083R	Prior to version 2.23.00	Version 2.23.00 and later
XNV-C9083R	Prior to version 2.23.00	Version 2.23.00 and later
XNO-C8083R	Prior to version 2.23.00	Version 2.23.00 and later
XNO-C9083R	Prior to version 2.23.00	Version 2.23.00 and later
XNP-9250R	Prior to version 2.23.00	Version 2.23.00 and later
XNP-8250R	Prior to version 2.23.00	Version 2.23.00 and later

XNP-9250	Prior to version 2.23.00	Version 2.23.00 and later
XNP-8250	Prior to version 2.23.00	Version 2.23.00 and later
XNP-6400R	Prior to version 2.23.00	Version 2.23.00 and later
XNP-6400	Prior to version 2.23.00	Version 2.23.00 and later
XNP-9300RW	Prior to version 2.23.00	Version 2.23.00 and later
XNP-8300RW	Prior to version 2.23.00	Version 2.23.00 and later
XNP-6400RW	Prior to version 2.23.00	Version 2.23.00 and later
TNV-C7013RC	Prior to version 2.23.00	Version 2.23.00 and later
XNP-C6403	Prior to version 2.23.00	Version 2.23.00 and later
XNP-C6403R	Prior to version 2.23.00	Version 2.23.00 and later
XNP-C6403RW	Prior to version 2.23.00	Version 2.23.00 and later
XNP-C8253	Prior to version 2.23.00	Version 2.23.00 and later
XNP-C8253R	Prior to version 2.23.00	Version 2.23.00 and later
XNP-C8303RW	Prior to version 2.23.00	Version 2.23.00 and later
XNP-C9253	Prior to version 2.23.00	Version 2.23.00 and later
XNP-C9253R	Prior to version 2.23.00	Version 2.23.00 and later
XNP-C9303RW	Prior to version 2.23.00	Version 2.23.00 and later
XNO-6123R	Prior to version 2.23.00	Version 2.23.00 and later
XNV-6123R	Prior to version 2.23.00	Version 2.23.00 and later
XNB-8002	Prior to version 2.23.00	Version 2.23.00 and later
XNB-9002	Prior to version 2.23.00	Version 2.23.00 and later
XND-8082RF	Prior to version 2.23.00	Version 2.23.00 and later
XND-8082RV	Prior to version 2.23.00	Version 2.23.00 and later
XND-9082RF	Prior to version 2.23.00	Version 2.23.00 and later
XND-9082RV	Prior to version 2.23.00	Version 2.23.00 and later
XNO-8082R	Prior to version 2.23.00	Version 2.23.00 and later
XNO-9082R	Prior to version 2.23.00	Version 2.23.00 and later
XNV-8082R	Prior to version 2.23.00	Version 2.23.00 and later
XNV-9082R	Prior to version 2.23.00	Version 2.23.00 and later
XNP-C9310R	Prior to version 2.23.00	Version 2.23.00 and later
XNF-9010RV	Prior to version 2.23.00	Version 2.23.00 and later
XNF-9010RVM	Prior to version 2.23.00	Version 2.23.00 and later
XNF-9010RS	Prior to version 2.23.00	Version 2.23.00 and later
XNF-9013RV	Prior to version 2.23.00	Version 2.23.00 and later

■ 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.