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

2023 Hanwha Vision S-Cert Team

Camera Vulnerability Report

■ OVERVIEW

- IPVM (Bashis) found these three vulnerabilities in Hanwha cameras and reported to Hanwha S-CERT at February 7th, 2023.

Vulnerability	Description
Authenticated Command Injection	Randomly injecting a command into the folder mount point of the NAS function and executing a Linux command
DoS of WS Discovery and Hanwha proprietary discovery services	After injecting EMPTY packets into the 3702 / 7701 ports used for device discovery of ONVIF/Device Manager, the discovery function can be disabled
Authenticated XSS	Can be executed by injecting the script into the imageData/backupfileData parameters of /home/setup/imagedownload.cgi

■ AFFECTED PRODUCTS AND FIRMWARE

- You can refer below tables for affected series, affected firmware version, corrected firmware version

Model		Affected Firmware Version	Corrected Firmware Version
A Series		1.41.02 and earlier versions	1.41.03 and later versions
Q Series	2M	1.41.13 and earlier versions	1.41.14 and later versions
	Others	1.41.04 and earlier versions	1.41.05 and later versions
PNM Series		1.33.03 and earlier versions 2.21.01 and earlier versions	2.22.00 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

■ RISK ANALYSIS

Vulnerability	Review Opinion	Severity
Authenticated Command Injection	Hanwha was filtering special characters in the DefaultFolder factor used for the NAS function, but it was confirmed that the command could be executed due to the missing special character'$' **However, this vulnerability requires authentication before it can be executed.**	Middle
DoS of WS Discovery and Hanwha proprietary discovery services	**Even if a DoS attack occurs, service limitations occur only in the discovery function to find products on the local network, not in all services of Hanwha Products.** **RISK MITIGATION** In situations where there is a DoS attack and the firmware cannot be updated, rebooting the device can temporarily solve the problem. **※ Only, this vulnerability affects all Hanwha products.** So, all Hanwha products has being released corrected firmware. (Refer to the #1)	Low
Authenticated XSS	**It is difficult to exploit because it is very difficult to run on the actual browser. Also, even if js is executed, no additional benefits are obtained.** **This vulnerability requires authentication as well before it can be exploited.**	Low

■ Current Status and Required Action

- Regardless of the severity of the vulnerabilities discovered, Hanwha Vision has resolved these vulnerabilities by releasing corrected firmware.
- Please, update those affected models with latest firmware.

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

#1. Release Plan for DoS of WS Discovery and Hanwha proprietary discovery services

Model	Affected Firmware Version	Corrected Firmware Version
P Series	2.11.03 and earlier versions	2.12.00 and later versions
X Series	2.21.00 and earlier versions	2.22.00 and later versions
T Series	2.11.11 and earlier versions	2.12.00 and later versions
L Series	1.41.11 and earlier versions	1.41.12 and later versions
Encoder	2.11.03 and earlier versions	2.21.01 and later versions