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

4/26/2023

5/15/2023 (Updated)

Camera Vulnerability Report (CVE-2023-31994 ~ 31996)

■ OVERVIEW

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

CVE	Description
CVE-2023-31994	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. Service limitations occur only in the discovery function.
CVE-2023-31995	Authenticated XSS Can be executed by injecting the script into the imageData/backupfileData parameters of /home/setup/imagedownload.cgi
CVE-2023-31996	Authenticated Command Injection Randomly injecting a command into the folder mount point of the NAS function and executing a Linux command

■ AFFECTED PRODUCTS AND FIRMWARE

- The vulnerability **CVE-2023-31994** affects all current Hanwha camera and encoder models.
- The vulnerabilities **CVE-2023-31995 & CVE-2023-31996** affect the following camera series. You can refer to the below table for the affected series, affected firmware version, and corrected firmware version

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

Model		Affected Firmware Version	Corrected Firmware Version
A Series		1.41.02 and earlier versions	1.41.03 and later versions
Q Series	Basic 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

■ RISK ANALYSIS

CVE	Review Opinion	Severity
CVE-2023-31994	**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 have corrected firmware released. (Refer to the section "Release Plan for CVE-2023-31994" below.)	Low
CVE-2023-31995	**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 also requires authentication before it can be exploited, so the scope and severity is limited.**	Low
CVE-2023-31996	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 missing the special character'$' **This vulnerability requires authentication before it can be executed, so the scope and severity is limited.**	Middle

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

■ 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 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 the Hanwha Vision website.
- 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.

■ Release Plan for CVE-2023-31994

➢ In addition to Hanwha A, Q, and PNM Series, Hanwha P, X, T, L Series and Encoders have been updated for **CVE-2023-31994**, but are not affected by **CVE-2023-31995**, **CVE-2023-31996** vulnerabilities. The below table lists the updated firmware versions to resolve this vulnerability.

Model		Affected Firmware Version	Corrected Firmware Version	CVE-2023-31995 CVE-2023-31996
P Series		2.11.03 and earlier versions	2.12.00 and later versions	Not Affected
X Series		2.21.00 and earlier versions	2.22.00 and later versions	Not Affected
T Series		2.11.11 and earlier versions	2.12.00 and later versions	Not Affected
L Series		1.41.11 and earlier versions	1.41.12 and later versions	Not Affected
Encoders		2.11.03 and earlier versions	2.21.01 and later versions	Not Affected
A Series		1.41.02 and earlier versions	1.41.03 and later versions	Affected
Q Series	Basic 2M	1.41.13 and earlier versions	1.41.14 and later versions	Affected
	Others	1.41.04 and earlier versions	1.41.05 and later versions	Affected
PNM Series		1.33.03 and earlier versions 2.21.01 and earlier versions	2.22.00 and later versions	Affected