Hanwha Techwin
6, Pangyo-ro 319 beon-gil, bundang-gu, Seongman-si, Gyeonggi-do, 463-400 Rep. of KOREA
TEL 82.70.7147.8753 FAX 82.31.8018.3740 www.hanwha-security.com

2019 Hanwha Techwin S-Cert Team

NVR Vulnerability Report (CVE-2019-12223)

■ OVERVIEW

- Vulnerability : Buffer overflow (CVE-2019-12223)
- Description

  The listed NVR is vulnerable to allow remote attackers to cause a denial of service (such as system crash and reboot) using buffer overflow.

■ AFFECTED PRODUCTS AND FIRMWARE

Model	Firmware Version	Status	Remarks
SRN-1000	V1.52 and earlier versions	No plan	Discontinued
SRN-1670D	V2.04 and earlier versions	No plan	Discontinued
SRN-470D	V2.04 and earlier versions	No plan	Discontinued
SRN-1673S	V1.16 and earlier versions	Resolved (V1.18_190916)	Discontinued
SRN-873S	V1.16 and earlier versions	Resolved (V1.18_190916)	Discontinued
SRN-473S	V1.16 and earlier versions	Resolved (V1.18_190916)	Discontinued
SRN-472S	V1.06 and earlier versions	Resolved (V1.08_190614)	Discontinued
SRN-4000	V2.20 and earlier versions	Resolved (V2.22_190923)	Discontinued

■ RISK ANALYSIS

Vulnerability	Review Result	Severity
Buffer overflow (CVE-2019-12223)	The NVR can be rebooted via external attack continuously if it can be access via the public network. During the time, video transmission and recording will not be operated. Also, Exploiting the vulnerability is trivial and requires very low skill level.	High

■ Current Status & Plan

Hanwha Techwin
6, Pangyo-ro 319 beon-gil, bundang-gu, Seongman-si, Gyeonggi-do, 463-400 Rep. of KOREA
TEL 82.70.7147.8753 FAX 82.31.8018.3740 www.hanwha-security.com

- The listed all models are currently discontinued. Nevertheless, Hanwha Techwin have released the patched firmware regarding SRN-472S, 473S, 873S, 1673S, 4000 models.
- However, SRN-1000, 1670D, 470D models will not be updated any more due to the date of discontinuation and End Of Life.

■ Required Action

- SRN-472S, 473S, 873S, 1673S, 4000 models, update NVR immediately with latest firmware.
- As SRN-1000, 1670D, 470D models have no patched firmware, NVR needs to be disconnected from the public network or be blocked from untrusted IPs using IP firewall.