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 한화테크윈 S-Cert팀

NVR 취약점 리포트 (CVE-2019-12223)

■ 개요

- 취약점 명 : 버퍼 오버플로우 (CVE-2019-12223)
- 취약점 설명

  하기 언급된 NVR에 원격 공격자가 버퍼 오버플로우를 사용하여 서비스 거부(예: 시스템 충돌 및 재부팅)를 유발시킬 수 있는 취약점이 발견되었습니다.

■ 영향받는 제품 및 펌웨어 버전

모델명	펌웨어 버전	상태	비고
SRN-1000	V1.52 이하 버전	계획 없음	단종
SRN-1670D	V2.04 이하 버전	계획 없음	단종
SRN-470D	V2.04 이하 버전	계획 없음	단종
SRN-1673S	V1.16 이하 버전	해결됨 (V1.18_190916)	단종
SRN-873S	V1.16 이하 버전	해결됨 (V1.18_190916)	단종
SRN-473S	V1.16 이하 버전	해결됨 (V1.18_190916)	단종
SRN-472S	V1.06 이하 버전	해결됨 (V1.08_190614)	단종
SRN-4000	V2.20 이하 버전	해결됨 (V2.22_190923)	단종

■ 리스크 분석

보안 취약점	리뷰 결과	심각도
버퍼 오버플로우 (CVE-2019-12223)	NVR 이 공용 네트워크를 통해 접근 가능한 경우 지속적인 외부 공격으로 재부팅될 수 있으며, 재부팅 시간 동안 영상 전송 및 녹화가 불가능하게 됩니다. 또한 해당 취약점은 간단한 기술만으로도 쉽게 공격이 가능합니다.	높음

■ 현상태 및 계획

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

- 언급된 모든 모델들은 3년전에 단종된 상태입니다만, 당사는 SRN-472S, 473S, 873S, 1673S, 4000 모델에 대하여 패치 펌웨어를 배포하였습니다.
- 그러나, SRN-1000, 1670D, 470D 모델은 오래 전에 단종(제품의 수명 종료)되어 더 이상 패치 펌웨어를 배포할 수 없습니다.

■ 필요한 조치

- SRN-472S, 473S, 873S, 1673S, 4000 모델은 즉시 NVR을 최신 펌웨어로 업데이트하시기 바랍니다.
- SRN-1000, 1670D, 470D 모델은 패치된 펌웨어가 존재하지 않으므로 공용 네트워크로부터 연결된 NVR을 분리하거나 IP 방화벽을 사용하여 신뢰할 수 없는 IP로부터 차단하는 것이 필요합니다.