합동분석협의체 보안권고문

보안취약 CCTV 보안권고문

2023. 4. 25

❶ 개 요

- 최근 Hikvision CCTV 제품 대상 공개 취약점(권한상승, 커맨드 인젝션 등 2종)·기본 비밀번호 등 악용한 해킹사고 발생
- 이에, 취약점 공격으로 인해 추가 피해발생이 우려됨에 따라 기본 비밀번호 변경·펌웨어 보안업데이트를 권고하고 탐지 규칙(Snort Rule) 등 배포

❷ 보안업데이트 권고

- 제조사 홈페이지(https://www.hikvision.com/en/support/download/firmware/)를 방문, 취약한 모델·버전(아래 표 참조) 대상 최신 펌웨어 업데이트 실시

  - 펌웨어 업데이트 전까지 인터넷 연결 차단 후 운용 권고

취약점	제품모델	취약버전
CVE-2017-7921	DS-2CD2xx2F-I Series	140721 ~ 160530 빌드 버전
	DS-2CD2xx0 Series	140721 ~ 161107 빌드 버전
	DS-2CD4x2xFWD Series	140721 ~ 160414 빌드 버전
	DS-2CD4xx5 Series	140721 ~ 160421 빌드 버전
	DS-2CD2xx2FWD Series	150410 ~ 161125 빌드 버전
	DS-2DEx Series	140807 ~ 150910 빌드 버전
	DS-2DFx Series	140805 ~ 160928 빌드 버전
CVE-2021-36260	DS-2CVxxx1 DS-2CVxxx6 HWI-xxxx IPC-xxxx DS-2CD1xx1 DS-2CD1x23G0E(C) DS-2CD1x43(B) DS-2CD1x43(C) DS-2CD1x43G0E DS-2CD1x53(B) DS-2CD1x53(C) DS-2CD1xx7G0 DS-2CD2xx6G2 DS-2CD2xx6G2(C) DS-2CD2xx7G2 DS-2CD2xx7G2(C) DS-2CD2x21G0(C) DS-2CD2x21G1(C)	210625 이전 빌드 버전

	DS-2CD2xx3G2 DS-2CD3xx6G2 DS-2CD3xx6G2(C) DS-2CD3xx7G2 DS-2CD3xx7G2(C) DS-2CD3xx7G0E DS-2CD3x21G0 DS-2CD3x21G0(C) DS-2CD3x51G0(C) DS-2CD3xx3G2 DS-2CD4xx0 DS-2CD4xx6 iDS-2XM6810 iDS-2CD6810 DS-2XE62x2F(D) DS-2XC66x5G0 DS-2XE64x2F(B) DS-2CD8Cx6G0 iDS-2PTxxxx iDS-2SE7xxxx DS-2DYHxxxx DS-2DY9xxxx PTZ-Nxxxx HWP-Nxxxx DS-2DF5xxxx DS-2DF6xxxx DS-2DF6xxxx-Cx DS-2DF7xxxx DS-2DF8xxxx DS-2DF9xxxx iDS-2PT9xxxx iDS-2SK7xxxx iDS-2SK8xxxx iDS-2SR8xxxx iDS-2VSxxxx	
	DS-2TBxxx DS-Bxxxx DS-2TDxxxxB DS-2TD1xxx-xx DS-2TD2xxx-xx DS-2TD41xx-xx/Wx DS-2TD62xx-xx/Wx DS-2TD81xx-xx/Wx DS-2TD4xxx-xx/V2 DS-2TD62xx-xx/V2 DS-2TD81xx-xx/V2	210702 이전 빌드 버전
	DS-76xxNI-K1xx(C) DS-76xxNI-Qxx(C) DS-HiLookI-NVR-1xxMHxx-C(C) DS-HiLookI-NVR-2xxMHxx-C(C) DS-HiWatchI-HWN-41xxMHxx(C) DS-HiWatchI-HWN-42xxMHxx(C)	201224 ~ 210511 빌드 버전
	DS-71xxNI-Q1xx(C) DS-HiLookI-NVR-1xxMHxx-D(C) DS-HiLookI-NVR-1xxHxx-D(C) DS-HiWatchI-HWN-21xxMHxx(C) DS-HiWatchI-HWN-21xxHxx(C)	210221 ~ 210511 빌드 버전
	DS-2CD1x23G0 DS-2CD2xx1G0 DS-2CD2xx1G1 DS-2CD2x27G1 DS-2CD2x27G3E DS-2CD4xx6FWD (Non-ANPR) DS-2CD4xx5G0 DS-2XE6xx5G0 DS-2XE6xx2F DS-2XM6xx2FWD DS-2XM6xx2G0 iDS-2DExxxx	V5.5.0 보다 낮은 버전

• 공공분야의 경우 CCTV 도입 및 운영 관련「국가정보보안기본지침」및「국가·공공기관 영상정보 처리기기 도입·운영 가이드라인」등 보안대책 준수

❸ 탐지규칙

취약점	탐지 규칙(Snort Rule)
CVE-2017-7921	alert tcp any any -> any any (msg:"CVE-2017-7921"; flow:to_server; content:"/Security/users?auth=YWRtaW46MTEK"; sid:1;)
	alert tcp any any -> any any (msg:"CVE-2017-7921.A"; flow:to_server; content:"/onvif-http/snapshot?auth=YWRtaW46MTEK"; sid:2;)
	alert tcp any any -> any any (msg:"CVE-2017-7921.B"; flow:to_server; content:"/System/configurationFile?auth=YWRtaW46MTEK"; sid:3;)
CVE-2021-36260	alert tcp any any -> any 80 (msg:"CVE-2021-36260"; flow:to_server; content:"/SDK/webLanguage"; depth:150; fast_pattern; content:"|3C 6C 61 6E 67 75 61 67 65 3E 24 28|"; distance:0; content:")</language>"; distance:0; sid:4;)

. 끝.