

2018 Hanwha Techwin S-Cert Team

## DVR 취약점 리포트 (CVE-2018-11689)

### ■ 개요

- 취약점 명 : XSS - Cross Site Scripting (CVE-2018-11689)
- 취약점 설명

DVR에서 사용되는 웹뷰어는 사용자 입력 값의 불충분한 검증으로 인해 XSS 취약점에 노출되어 있습니다. 공격자는 조작된 인자 값이 포함된 URL 클릭을 유도하여, 사용자의 웹 브라우저에서 임의의 스크립트를 실행 시킬 수 있습니다.

### ■ 영향받는 제품 및 펌웨어 버전

모델명	펌웨어 버전	상태
HRD-1642	v1.16 이하 버전	해결됨 (1.20_181206)
HRD-842	v1.16 이하 버전	해결됨 (1.20_181206)
HRD-442	v1.16 이하 버전	해결됨 (1.20_181206)
HRD-1641	v1.14 이하 버전	해결됨 (1.20_181206)
HRD-841	v1.14 이하 버전	해결됨 (1.20_181206)
HRD-840	v1.14 이하 버전	해결됨 (1.20_181206)
HRD-440	v1.14 이하 버전	해결됨 (1.20_181206)
HRD-443	v1.14 이하 버전	해결중
SRD-1694U	v1.14 이하 버전	해결중

### ■ 리스크 분석

보안 취약점	리뷰 결과	심각도
Cross Site Scripting (CVE-2018-11689)	공격대상자는 DVR 웹뷰어에 로그인 한 상태에서 조작된 URL 을 클릭해야 합니다. 또한, 사용자의 인증 값이 암호화되고, DVR 의 웹 서버에서 검증되고 있기 때문에 권한도용, 인증값 노출 등의 피해를 발생 시킬 수 없습니다.	낮음



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

## ■ 현상태 및 계획

- 발견된 취약점의 영향도와 관계없이 한화테크윈은 본 XSS 취약점에 대해 URL의 사용자 입력 값을 필터링하고 검증하는 방식으로 개선하였습니다.
- 특정 타겟형인 HRD-443과 SRD-1694U 모델은 2019년 5월 배포 계획으로 개선 진행중입니다.