

2018 Hanwha Techwin S-Cert Team

## DVR Vulnerability Report (CVE-2018-11689)

### OVERVIEW

- Vulnerability : XSS - Cross Site Scripting (CVE-2018-11689)
- Description

The DVR web viewer is vulnerable to cross-site scripting caused by improper validation of URL. An attacker could exploit this vulnerability by crafting a URL to execute an arbitrary script in the victim's web browser once the URL is clicked.

### AFFECTED PRODUCTS AND FIRMWARE

Model	Firmware Version
HRD-1642	v1.16 and earlier versions
HRD-842	v1.16 and earlier versions
HRD-442	v1.16 and earlier versions
HRD-1641	v1.14 and earlier versions
HRD-841	v1.14 and earlier versions
HRD-840	v1.14 and earlier versions
HRD-440	v1.14 and earlier versions
HRD-443	v1.14 and earlier versions
SRD-1694U	v1.14 and earlier versions

### RISK ANALYSIS

Vulnerability	Review Result	Severity
Cross Site Scripting (CVE-2018-11689)	Victim's web page must be logged into the DVR and at the time they click the crafted URL in order for this vulnerability to be executed. Without this prerequisite attacker's crafted URL has no effect.	Low



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](http://www.hanwha-security.com)

## **Plan**

- Regardless of the vulnerability severity, Hanwha Techwin will reinforce the security of affected DVR devices. In this specific case, we will strengthen the web viewer logic to filter and validate URL input values.
- We will update firmware(v1.20) by November 30<sup>th</sup>, 2018.