Hanwha Techwin

Vulnerability Report

May 18, 2017

CVE-2017-7912 NVR Unauthenticated Access

OVERVIEW

A security research organization has discovered and disclosed a critical vulnerability in the firmware of certain Hanwha network video recording (NVR) devices. A specially crafted http request and response could allow an attacker to gain access to the device management page with admin privileges without proper authentication.

Firmware to address the exploit has been developed and released.

AFFECTED PRODUCTS AND FIRMWARE

Hanwha SRN-4000 NVR firmware prior to v2.16_170401.zip
Hanwha SRN-1673S/873S/473S NVR firmware prior to v1.08_160811.zip

IMPACT

An attacker needs to use a computer that has previously been properly logged into a NVR in order to successfully exploit the vulnerability. Cached files stored in the computer from the previous sessions can trigger the exploit. Attacks to affected devices from a computer which have previously logged in are at immediate risk.

Gaining an administrator privileges in Hanwha product provides the attacker with complete system access and the potential for them to read or delete the recordings, add new users, or any other actions the admin has access to.

An attacker will not be able to exploit the affected devices with this vulnerability with a computer that has never properly accessed the affected Hanwha devices.

RECOMMENDATIONS

Hanwha recommends to upgrade all affected products.

MITIGATION / FIRMWARE RELEASE

The latest firmware which addresses the vulnerability can be obtained from the following location:

https://www.hanwha-security.com

SRN-4000: (Products > Video Recorders > SRN-4000 > Download > Firmware)
SRN-1673S: (Products > Video Recorders > SRN-1673S > Download > Firmware)
SRN-873S: (Products > Video Recorders > SRN-873S > Download > Firmware)
SRN-473S: (Products > Video Recorders > SRN-473S > Download > Firmware)

6, Pangyo-ro 319beon-gil, Bundang-gu, Seongnam-si, Gyeonggi-do, 13488, Korea
TEL 8270.7147.7679 FAX 8231.8018.3711