Securing Video Surveillance Devices to Close Network Vulnerabilities

Hanwha
Techwin America

Aaron Saks
Product & Technical Manager
Hanwha Techwin America

Agenda

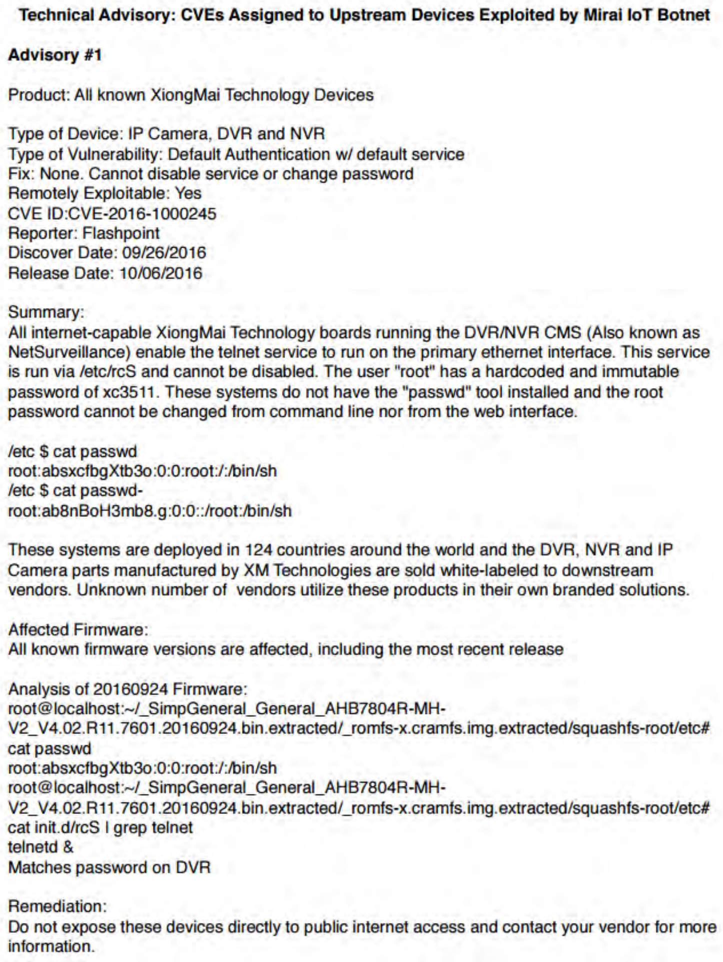
- State of the video cyber security industry
- What Hanwha is doing about these cyber security threats
- Discussion of key cyber security measures to implement in Hanwha products

It has been a very busy year in the (in)security world…

- Here is a recap and brief discussion of these events and how they relate to use, as well as the consequences of these events.

VMS removes support for “untrustworthy network devices”.

Requires end-user to sign liability release and pay extra license fee.



Technical Advisory: CVEs Assigned to Upstream Devices Exploited by Mirai IoT Botnet

Advisory #1

Product: All known XiongMai Technology Devices

Type of Device: IP Camera, DVR and NVR
Type of Vulnerability: Default Authentication w/ default service
Fix: None. Cannot disable service or change password
Remotely Exploitable: Yes
CVE ID:CVE-2016-1000245
Reporter: Flashpoint
Discover Date: 09/26/2016
Release Date: 10/06/2016

Summary:
All internet-capable XiongMai Technology boards running the DVR/NVR CMS (Also known as NetSurveillance) enable the telnet service to run on the primary ethernet interface. This service is run via /etc/rcS and cannot be disabled. The user "root" has a hardcoded and immutable password of xc3511. These systems do not have the "passwd" tool installed and the root password cannot be changed from command line nor from the web interface.

```
/etc $ cat passwd
root:absxcfbgXtb3o:0:0:root:/:/bin/sh
/etc $ cat passwd-
root:ab8nBoH3mb8.g:0:0::/root:/bin/sh
```

These systems are deployed in 124 countries around the world and the DVR, NVR and IP Camera parts manufactured by XM Technologies are sold white-labeled to downstream vendors. Unknown number of vendors utilize these products in their own branded solutions.

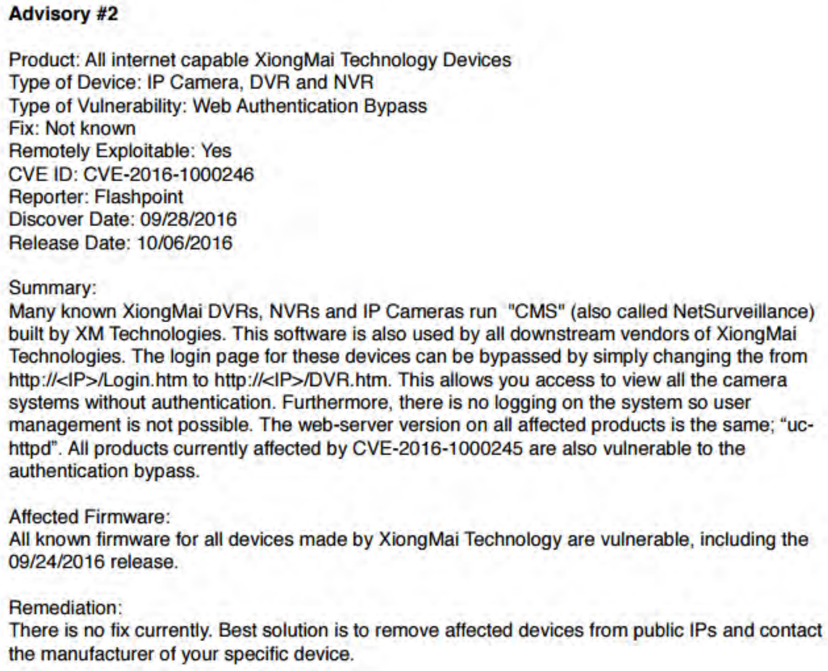
Affected Firmware:
All known firmware versions are affected, including the most recent release

Analysis of 20160924 Firmware:

```
root@localhost:~/_SimpGeneral_General_AHB7804R-MH-
V2_V4.02.R11.7601.20160924.bin.extracted/_romfs-x.cramfs.img.extracted/squashfs-root/etc#
cat passwd
root:absxcfbgXtb3o:0:0:root:/:/bin/sh
root@localhost:~/_SimpGeneral_General_AHB7804R-MH-
V2_V4.02.R11.7601.20160924.bin.extracted/_romfs-x.cramfs.img.extracted/squashfs-root/etc#
cat init.d/rcS l grep telnet
telnetd &
```

Matches password on DVR

Remediation:
Do not expose these devices directly to public internet access and contact your vendor for more information.



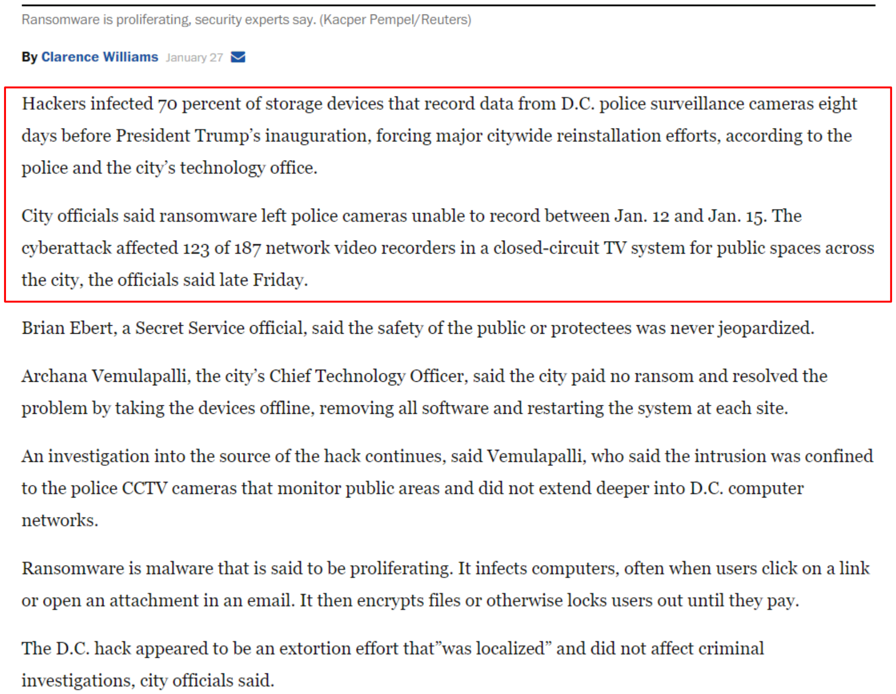
Advisory #2

Product: All internet capable XiongMai Technology Devices
Type of Device: IP Camera, DVR and NVR
Type of Vulnerability: Web Authentication Bypass
Fix: Not known
Remotely Exploitable: Yes
CVE ID: CVE-2016-1000246
Reporter: Flashpoint
Discover Date: 09/28/2016
Release Date: 10/06/2016

Summary:
Many known XiongMai DVRs, NVRs and IP Cameras run "CMS" (also called NetSurveillance) built by XM Technologies. This software is also used by all downstream vendors of XiongMai Technologies. The login page for these devices can be bypassed by simply changing the from http://<IP>/Login.htm to http://<IP>/DVR.htm. This allows you access to view all the camera systems without authentication. Furthermore, there is no logging on the system so user management is not possible. The web-server version on all affected products is the same; “uc-httpd”. All products currently affected by CVE-2016-1000245 are also vulnerable to the authentication bypass.

Affected Firmware:
All known firmware for all devices made by XiongMai Technology are vulnerable, including the 09/24/2016 release.

Remediation:
There is no fix currently. Best solution is to remove affected devices from public IPs and contact the manufacturer of your specific device.



Ransomware is proliferating, security experts say. (Kacper Pempel/Reuters)

By Clarence Williams January 27

Hackers infected 70 percent of storage devices that record data from D.C. police surveillance cameras eight days before President Trump's inauguration, forcing major citywide reinstallation efforts, according to the police and the city's technology office.

City officials said ransomware left police cameras unable to record between Jan. 12 and Jan. 15. The cyberattack affected 123 of 187 network video recorders in a closed-circuit TV system for public spaces across the city, the officials said late Friday.

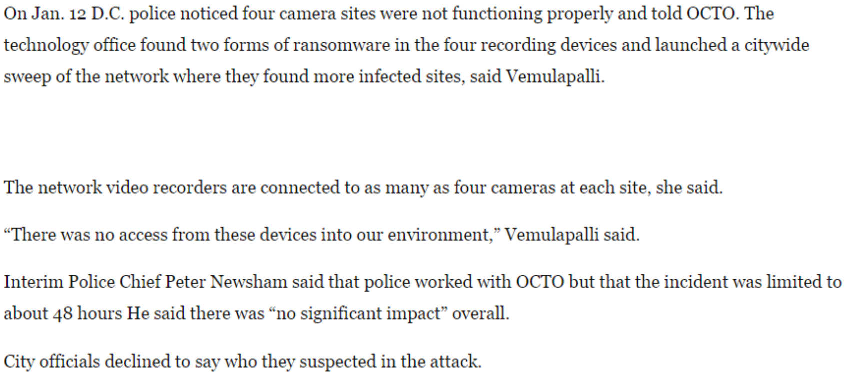
Brian Ebert, a Secret Service official, said the safety of the public or protectees was never jeopardized.

Archana Vemulapalli, the city's Chief Technology Officer, said the city paid no ransom and resolved the problem by taking the devices offline, removing all software and restarting the system at each site.

An investigation into the source of the hack continues, said Vemulapalli, who said the intrusion was confined to the police CCTV cameras that monitor public areas and did not extend deeper into D.C. computer networks.

Ransomware is malware that is said to be proliferating. It infects computers, often when users click on a link or open an attachment in an email. It then encrypts files or otherwise locks users out until they pay.

The D.C. hack appeared to be an extortion effort that"was localized" and did not affect criminal investigations, city officials said.



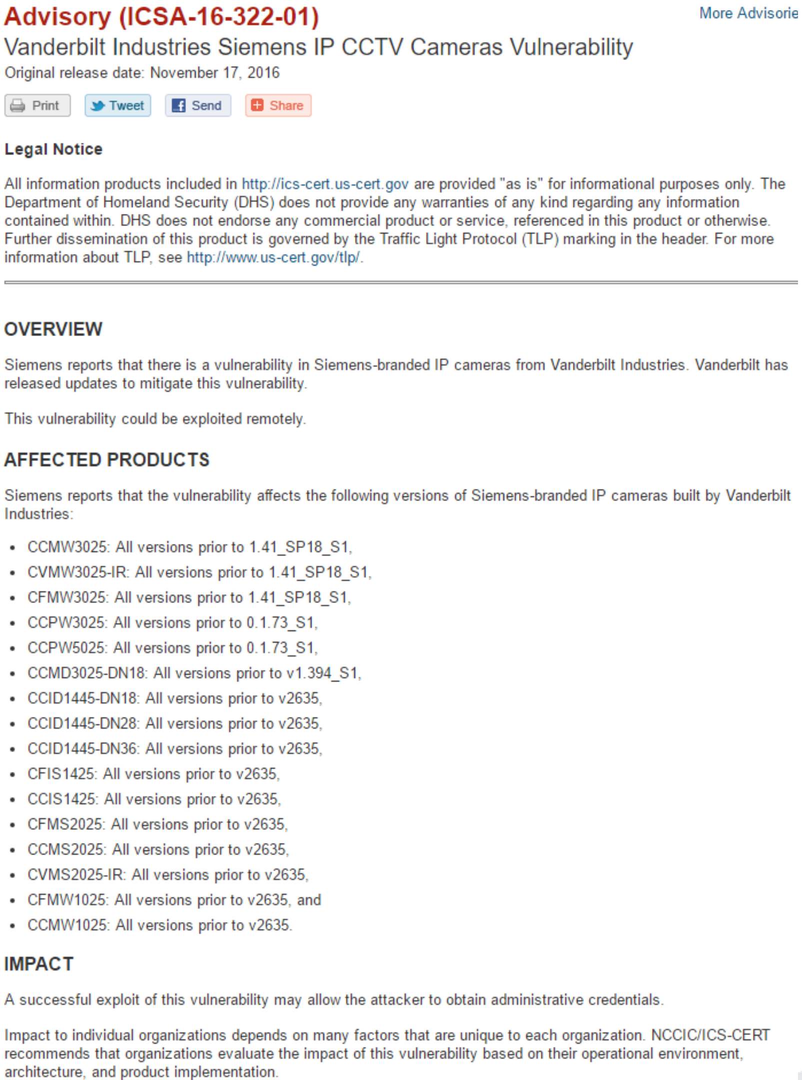
On Jan. 12 D.C. police noticed four camera sites were not functioning properly and told OCTO. The technology office found two forms of ransomware in the four recording devices and launched a citywide sweep of the network where they found more infected sites, said Vemulapalli.

The network video recorders are connected to as many as four cameras at each site, she said.

"There was no access from these devices into our environment," Vemulapalli said.

Interim Police Chief Peter Newsham said that police worked with OCTO but that the incident was limited to about 48 hours He said there was "no significant impact" overall.

City officials declined to say who they suspected in the attack.



Advisory (ICSA-16-322-01)

Vanderbilt Industries Siemens IP CCTV Cameras Vulnerability

Original release date: November 17, 2016

Legal Notice

All information products included in http://ics-cert.us-cert.gov are provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. DHS does not endorse any commercial product or service, referenced in this product or otherwise. Further dissemination of this product is governed by the Traffic Light Protocol (TLP) marking in the header. For more information about TLP, see http://www.us-cert.gov/tlp/.

OVERVIEW

Siemens reports that there is a vulnerability in Siemens-branded IP cameras from Vanderbilt Industries. Vanderbilt has released updates to mitigate this vulnerability.

This vulnerability could be exploited remotely.

AFFECTED PRODUCTS

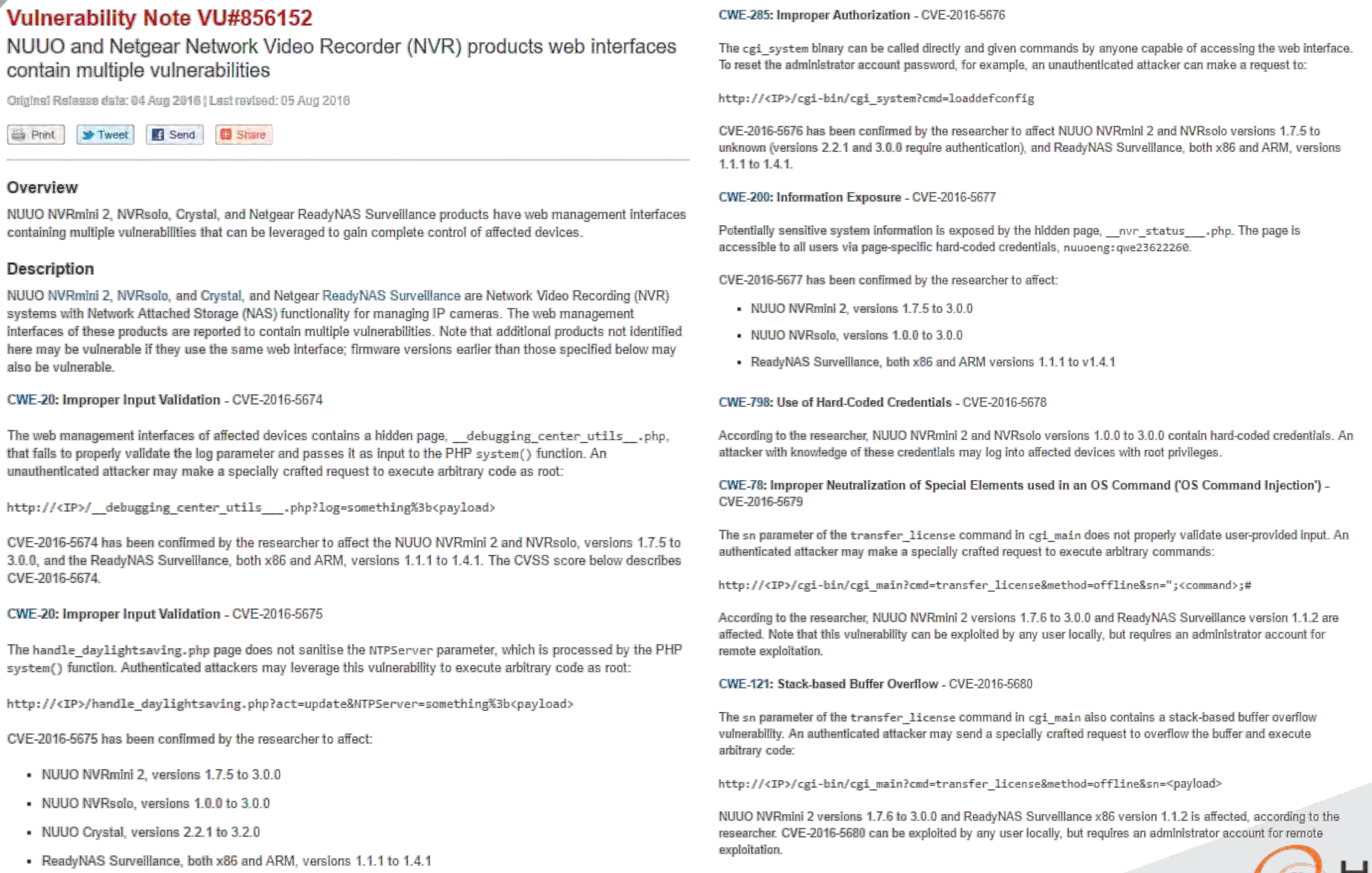
Siemens reports that the vulnerability affects the following versions of Siemens-branded IP cameras built by Vanderbilt Industries:

- CCMW3025: All versions prior to 1.41_SP18_S1,
- CVMW3025-IR: All versions prior to 1.41_SP18_S1,
- CFMW3025: All versions prior to 1.41_SP18_S1,
- CCPW3025: All versions prior to 0.1.73_S1,
- CCPW5025: All versions prior to 0.1.73_S1,
- CCMD3025-DN18: All versions prior to v1.394_S1,
- CCID1445-DN18: All versions prior to v2635,
- CCID1445-DN28: All versions prior to v2635,
- CCID1445-DN36: All versions prior to v2635,
- CFIS1425: All versions prior to v2635,
- CCIS1425: All versions prior to v2635,
- CFMS2025: All versions prior to v2635,
- CCMS2025: All versions prior to v2635,
- CVMS2025-IR: All versions prior to v2635,
- CFMW1025: All versions prior to v2635, and
- CCMW1025: All versions prior to v2635.

IMPACT

A successful exploit of this vulnerability may allow the attacker to obtain administrative credentials.

Impact to individual organizations depends on many factors that are unique to each organization. NCCIC/ICS-CERT recommends that organizations evaluate the impact of this vulnerability based on their operational environment, architecture, and product implementation.



Vulnerability Note VU#856152

NUUO and Netgear Network Video Recorder (NVR) products web interfaces contain multiple vulnerabilities

Original Release date: 04 Aug 2016 | Last revised: 05 Aug 2016

Overview

NUUO NVRmini 2, NVRsolo, Crystal, and Netgear ReadyNAS Surveillance products have web management interfaces containing multiple vulnerabilities that can be leveraged to gain complete control of affected devices.

Description

NUUO NVRmini 2, NVRsolo, and Crystal, and Netgear ReadyNAS Surveillance are Network Video Recording (NVR) systems with Network Attached Storage (NAS) functionality for managing IP cameras. The web management interfaces of these products are reported to contain multiple vulnerabilities. Note that additional products not identified here may be vulnerable if they use the same web interface; firmware versions earlier than those specified below may also be vulnerable.

CWE-20: Improper Input Validation - CVE-2016-5674

The web management interfaces of affected devices contains a hidden page, `__debugging_center_utils__.php`, that fails to properly validate the log parameter and passes it as input to the PHP `system()` function. An unauthenticated attacker may make a specially crafted request to execute arbitrary code as root:

```
http://<IP>/__debugging_center_utils___.php?log=something%3b<payload>
```

CVE-2016-5674 has been confirmed by the researcher to affect the NUUO NVRmini 2 and NVRsolo, versions 1.7.5 to 3.0.0, and the ReadyNAS Surveillance, both x86 and ARM, versions 1.1.1 to 1.4.1. The CVSS score below describes CVE-2016-5674.

CWE-20: Improper Input Validation - CVE-2016-5675

The `handle_daylightsaving.php` page does not sanitise the `NTPServer` parameter, which is processed by the PHP `system()` function. Authenticated attackers may leverage this vulnerability to execute arbitrary code as root:

```
http://<IP>/handle_daylightsaving.php?act=update&NTPServer=something%3b<payload>
```

CVE-2016-5675 has been confirmed by the researcher to affect:

- NUUO NVRmini 2, versions 1.7.5 to 3.0.0
- NUUO NVRsolo, versions 1.0.0 to 3.0.0
- NUUO Crystal, versions 2.2.1 to 3.2.0
- ReadyNAS Surveillance, both x86 and ARM, versions 1.1.1 to 1.4.1

CWE-285: Improper Authorization - CVE-2016-5676

The `cgi_system` binary can be called directly and given commands by anyone capable of accessing the web interface. To reset the administrator account password, for example, an unauthenticated attacker can make a request to:

```
http://<IP>/cgi-bin/cgi_system?cmd=loaddefconfig
```

CVE-2016-5676 has been confirmed by the researcher to affect NUUO NVRmini 2 and NVRsolo versions 1.7.5 to unknown (versions 2.2.1 and 3.0.0 require authentication), and ReadyNAS Surveillance, both x86 and ARM, versions 1.1.1 to 1.4.1.

CWE-200: Information Exposure - CVE-2016-5677

Potentially sensitive system information is exposed by the hidden page, `__nvr_status___.php`. The page is accessible to all users via page-specific hard-coded credentials, `nuuoeng:qwe23622260`.

CVE-2016-5677 has been confirmed by the researcher to affect:

- NUUO NVRmini 2, versions 1.7.5 to 3.0.0
- NUUO NVRsolo, versions 1.0.0 to 3.0.0
- ReadyNAS Surveillance, both x86 and ARM versions 1.1.1 to v1.4.1

CWE-798: Use of Hard-Coded Credentials - CVE-2016-5678

According to the researcher, NUUO NVRmini 2 and NVRsolo versions 1.0.0 to 3.0.0 contain hard-coded credentials. An attacker with knowledge of these credentials may log into affected devices with root privileges.

CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') - CVE-2016-5679

The `sn` parameter of the `transfer_license` command in `cgi_main` does not properly validate user-provided input. An authenticated attacker may make a specially crafted request to execute arbitrary commands:

```
http://<IP>/cgi-bin/cgi_main?cmd=transfer_license&method=offline&sn=";<command>;#
```

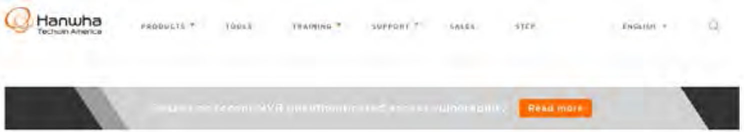
According to the researcher, NUUO NVRmini 2 versions 1.7.6 to 3.0.0 and ReadyNAS Surveillance version 1.1.2 are affected. Note that this vulnerability can be exploited by any user locally, but requires an administrator account for remote exploitation.

CWE-121: Stack-based Buffer Overflow - CVE-2016-5680

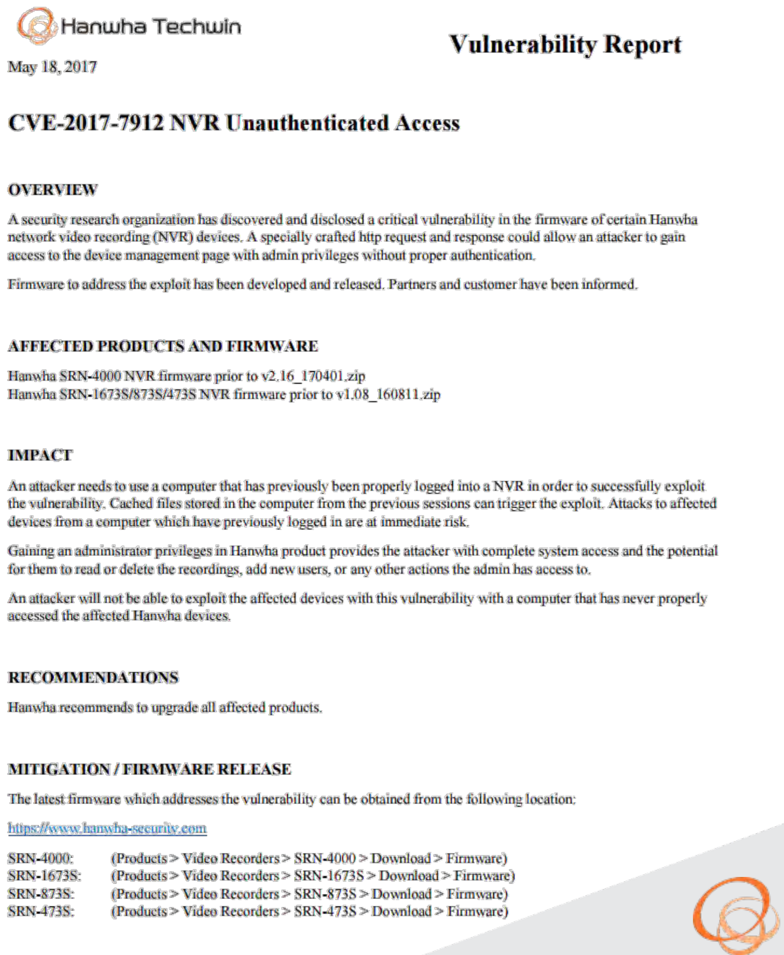
The `sn` parameter of the `transfer_license` command in `cgi_main` also contains a stack-based buffer overflow vulnerability. An authenticated attacker may send a specially crafted request to overflow the buffer and execute arbitrary code:

```
http://<IP>/cgi-bin/cgi_main?cmd=transfer_license&method=offline&sn=<payload>
```

NUUO NVRmini 2 versions 1.7.6 to 3.0.0 and ReadyNAS Surveillance x86 version 1.1.2 is affected, according to the researcher. CVE-2016-5680 can be exploited by any user locally, but requires an administrator account for remote exploitation.



[illegible] NVR unauthenticated access vulnerability.



Hanwha Techwin

May 18, 2017

Vulnerability Report

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. Partners and customer have been informed.

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:

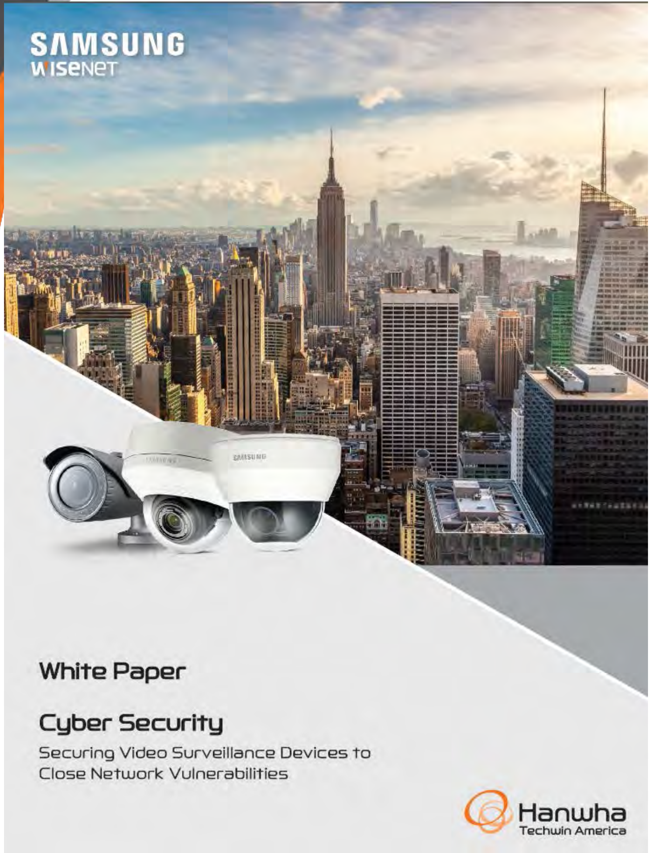
https://www.hanwha-security.com

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)

What is Hanwha Techwin doing to keep your systems safe and secure??

Hanwha
Techwin America

Hanwha – Cyber Security White Paper



White Paper

Cyber Security

Securing Video Surveillance Devices to Close Network Vulnerabilities

Hanwha
Techwin America

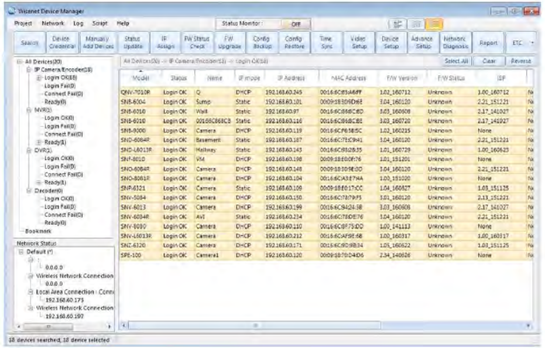
Introduction

We live in an increasingly connected world, where more and more devices and systems are networked and shared with other systems. Convenience is a main driver behind this trend, as people have come to expect the ability to connect to and control devices and systems anywhere, anytime.

However, there is a downside to the unprecedented level of convenience provided by the growing number of networked devices, namely increased security risk. Because each device is an endpoint for networks, they introduce the potential to become entry points for hackers and others with malicious intents. In fact, in many of the most high-profile data breaches that have occurred recently, hackers were able to access corporate networks through POS, HVAC and other networked systems that failed to provide an adequate level of security to prevent these types of breaches.

While IP-based video surveillance and other solutions have grown in popularity to become the accepted standard for new deployments and upgrades, security systems are no exception. A hacker does not discriminate among networked devices whether it performs a critical function like security or not. As such, video surveillance cameras and other devices are among the lengthy list of potential network entry points that are continually being probed for vulnerabilities that can be exploited. Therefore, it is essential that organizations take the necessary measures to ensure the highest level of security for their networks and IP cameras, encoders, NVRs and DVRs. There are a number of best practices that should be undertaken to strengthen device security to prevent unauthorized access and protect end users video surveillance systems and their overall network. Hanwha is not only aware of these best practices but has built a number of technologies and capabilities into its products to make it easier for organizations to take these important steps toward improving network security. These items should be reviewed by the owner of security systems, IT personnel, and Systems Integrators installing systems to determine the level of security needed while balancing the ease of use, with acceptable risks.

This guide will show snapshots from network cameras where applicable. Most settings can be configured in batch for multiple cameras using the Wisenet Device Manager Software (Figure 1).



Model	Status	Name	IP mode	IP Address	MAC Address	F/W Version	F/W Status	ISP
QNV-7010R	Login OK	Q	DHCP	192.168.60.245	00:16:6C:83:A6:FF	1.02_160712	Unknown	1.00_160712
SNB-6004	Login OK	Sump	Static	192.168.60.101	00:09:18:30:9D:6E	3.04_160120	Unknown	2.21_151221
SNB-6010	Login OK	Wall	Static	192.168.60.97	00:16:6C:86:8C:8D	3.03_160608	Unknown	2.17_141027
SNB-6010	Login OK	00166C868CB	Static	192.168.60.116	00:16:6C:86:8C:8E	3.03_160720	Unknown	2.17_141027
SNB-9000	Login OK	Camera	DHCP	192.168.60.119	00:16:6C:F6:3B:5C	1.02_160215	Unknown	None
SND-6084R	Login OK	Basement	Static	192.168.60.187	00:16:6C:75:C9:41	3.04_160120	Unknown	2.21_151221
SND-L6013R	Login OK	Hallway	Static	192.168.60.143	00:16:6C:93:2B:35	1.01_160729	Unknown	1.00_160623
SNF-8010	Login OK	VM	DHCP	192.168.60.198	00:09:18:E0:0F:76	1.01_151201	Unknown	None
SNO-6084R	Login OK	Camera	DHCP	192.168.60.148	00:09:18:30:9E:0D	3.04_160120	Unknown	2.21_151221
SNO-8081R	Login OK	Camera	DHCP	192.168.60.104	00:16:6C:A3:E7:4A	1.00_151020	Unknown	None
SNP-6321	Login OK	Camera	Static	192.168.60.109	00:09:18:E0:17:CC	1.04_160827	Unknown	1.03_151125
SNV-5084	Login OK	Camera	DHCP	192.168.60.150	00:16:6C:78:79:F5	3.01_160120	Unknown	2.13_151221
SNV-6013	Login OK	Camera	DHCP	192.168.60.199	00:16:6C:94:24:5B	3.03_160608	Unknown	2.17_141027
SNV-6084R	Login OK	AVI	Static	192.168.60.234	00:16:6C:78:DE:76	3.04_160120	Unknown	2.21_151221
SNV-8080	Login OK	Camera	DHCP	192.168.60.110	00:16:6C:8F:75:DD	1.00_141113	Unknown	None
SNV-L6013R	Login OK	Camera	DHCP	192.168.60.212	00:16:6C:AF:9E:6B	1.00_160317	Unknown	1.00_160317
SNZ-6320	Login OK	Camera	DHCP	192.168.60.171	00:16:6C:9D:9B:34	1.05_160622	Unknown	1.03_151125
SPE-100	Login OK	Camera1	DHCP	192.168.60.120	00:09:18:70:04:D6	2.34_140626	Unknown	None

18 devices searched, 18 device selected

Figure 1

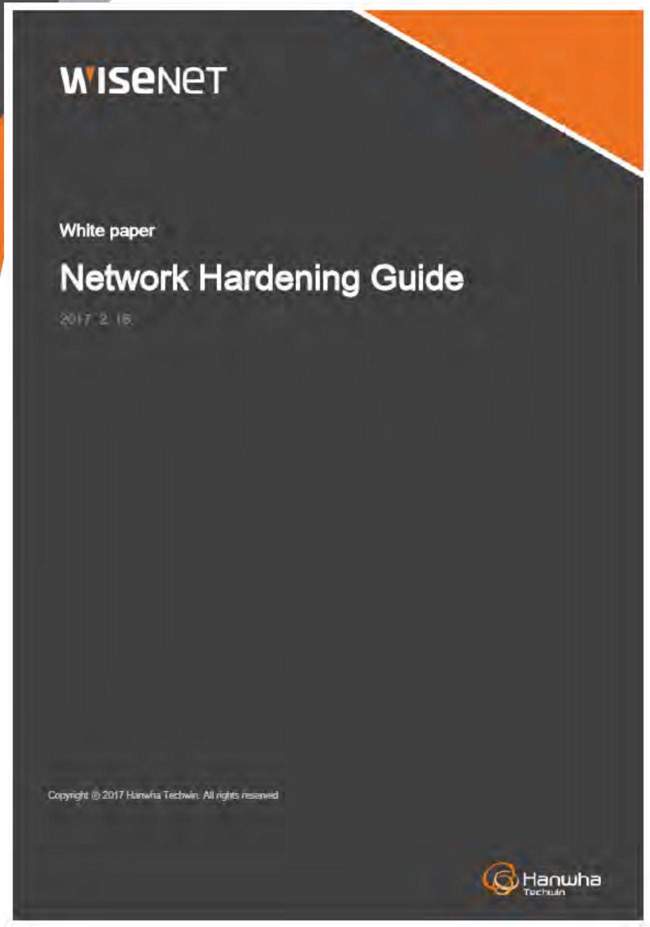
Summary

The harsh reality in today's connected world is that individuals and groups will continue their attempts to identify and exploit vulnerabilities to breach network security. And while we benefit from the convenience of a growing number of devices accessible via those networks, the reality is that those devices only increase the likelihood of unauthorized network access. Therefore, it is vital that all of these devices are secured to prevent them from becoming an open door for hackers. Employing these best practices not only can prevent networked video devices and systems from serving as entry points, but also ensures the integrity and continued operation of this critical function – ensuring the ongoing safety and security of people and assets. Additionally, many of these steps are also applicable to other devices and systems. Therefore, these best practices serve as a requirement for organizations that recognize the importance of and are serious about securing their networks.

Therefore, these best practices serve as a conversation starter for organizations that recognize the importance of and are serious about securing their networks. Open and informed dialogue between the end user, their IT department, the installer and systems integrator, are the key to finding the best solution to fit an individual organization's security needs.

Techwin America

Hanwha Techwin Network Hardening Guide



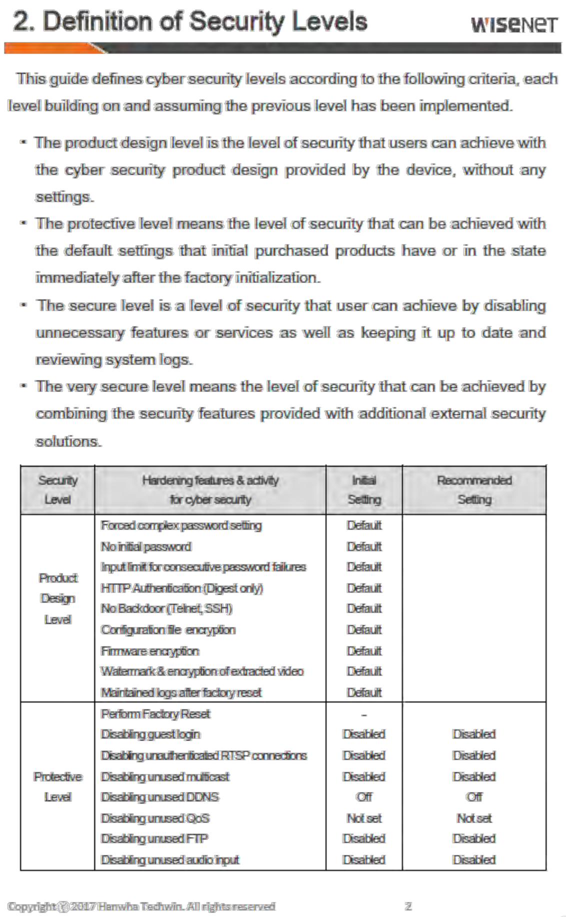
WISENET

White paper

Network Hardening Guide

2017. 2. 16.

Hanwha Techwin



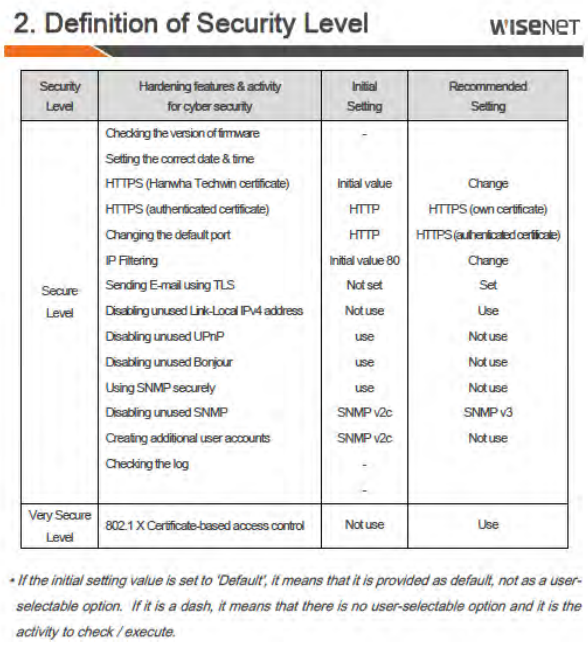
2. Definition of Security Levels

WISENET

This guide defines cyber security levels according to the following criteria, each level building on and assuming the previous level has been implemented.

- The product design level is the level of security that users can achieve with the cyber security product design provided by the device, without any settings.
- The protective level means the level of security that can be achieved with the default settings that initial purchased products have or in the state immediately after the factory initialization.
- The secure level is a level of security that user can achieve by disabling unnecessary features or services as well as keeping it up to date and reviewing system logs.
- The very secure level means the level of security that can be achieved by combining the security features provided with additional external security solutions.

Security Level	Hardening features & activity for cyber security	Initial Setting	Recommended Setting
Product Design Level	Forced complex password setting	Default	
	No initial password	Default	
	Input limit for consecutive password failures	Default	
	HTTP Authentication (Digest only)	Default	
	No Backdoor (Telnet, SSH)	Default	
	Configuration file encryption	Default	
	Firmware encryption	Default	
	Watermark & encryption of extracted video	Default	
	Maintained logs after factory reset	Default	
Protective Level	Perform Factory Reset	-	
	Disabling guest login	Disabled	Disabled
	Disabling unauthenticated RTSP connections	Disabled	Disabled
	Disabling unused multicast	Disabled	Disabled
	Disabling unused DDNS	Off	Off
	Disabling unused QoS	Not set	Not set
	Disabling unused FTP	Disabled	Disabled
	Disabling unused audio input	Disabled	Disabled



2. Definition of Security Level

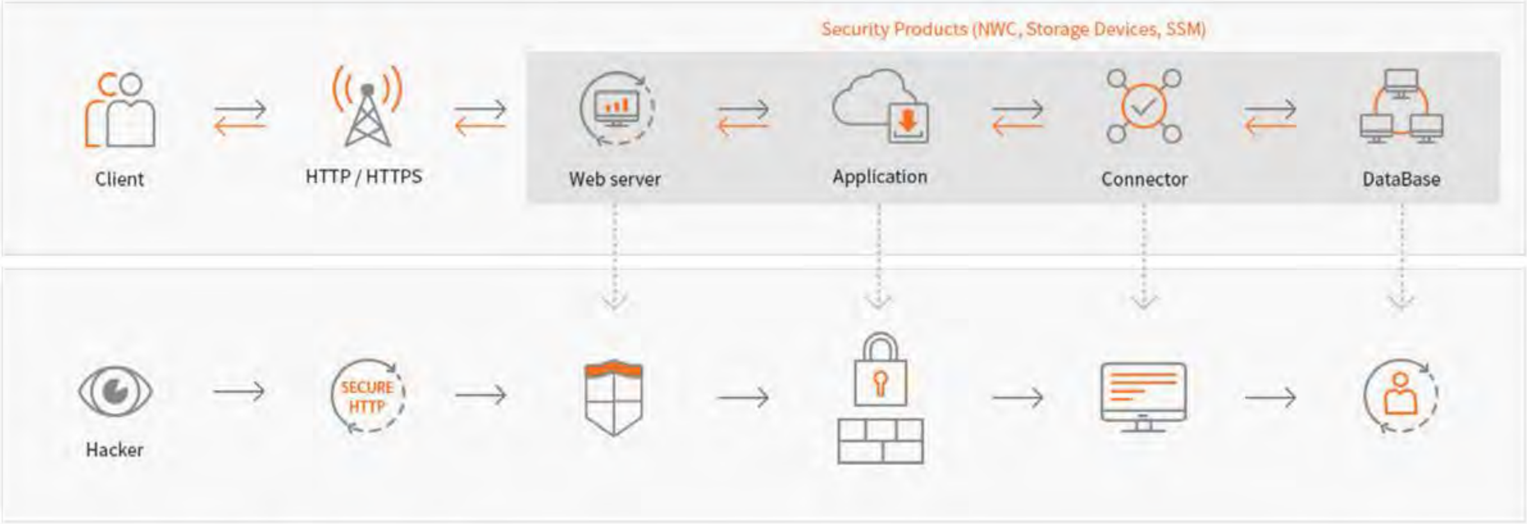
WISENET

Security Level	Hardening features & activity for cyber security	Initial Setting	Recommended Setting
Secure Level	Checking the version of firmware	-	
	Setting the correct date & time		
	HTTPS (Hanwha Techwin certificate)	Initial value	Change
	HTTPS (authenticated certificate)	HTTP	HTTPS (own certificate)
	Changing the default port	HTTP	HTTPS (authenticated certificate)
	IP Filtering	Initial value 80	Change
	Sending E-mail using TLS	Not set	Set
	Disabling unused Link-Local IPv4 address	Not use	Use
	Disabling unused UPnP	use	Not use
	Disabling unused Bonjour	use	Not use
	Using SNMP securely	use	Not use
	Disabling unused SNMP	SNMP v2c	SNMP v3
	Creating additional user accounts	SNMP v2c	Not use
	Checking the log	-	
		-	
Very Secure Level	802.1 X Certificate-based access control	Not use	Use

- *If the initial setting value is set to 'Default', it means that it is provided as default, not as a user-selectable option. If it is a dash, it means that there is no user-selectable option and it is the activity to check / execute.*

Hanwha Techwin America

Hanwha – Security by Design



Hacker Intrusion Prevention Technology

User authentication encryption (HTTPS encryption) Video transmission encryption (RTP-over-HTTPS, SRTP)

IP filtering, Daemon removal (Tablet, SSH)

Firmware encryption, password policy enforcement

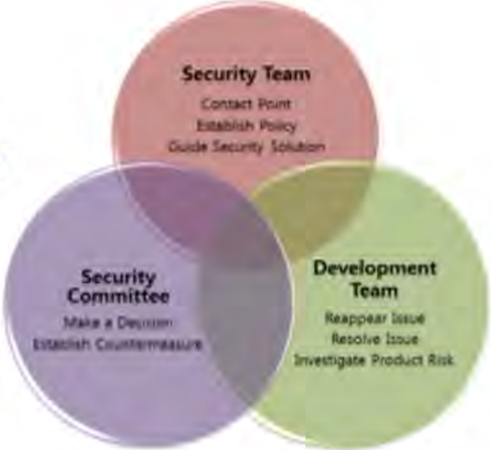
Secure coding

Personal information encryption (AES, SHA2)

Hanwha – Security by Design

□ Vulnerability Management Process

- After Action Process
  - Exclusive security team (S-CERT: secure.cctv@hanwha.com)
  - Response / After action to infringement by hacker
  - Role assign to Security Committee, S-CERT(Security Team), Development Team.



Various Press Media

Cybergibbons

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Improvement of vulnerabilities that reported from various organization (since 2012)

Cookies, User authentication, Backdoor, Firmware & video encryption, etc.

SAMSUNG SAMSUNG SDS

ZERO DAY INITIATIVE

KISA Korea Internet & Security Agency

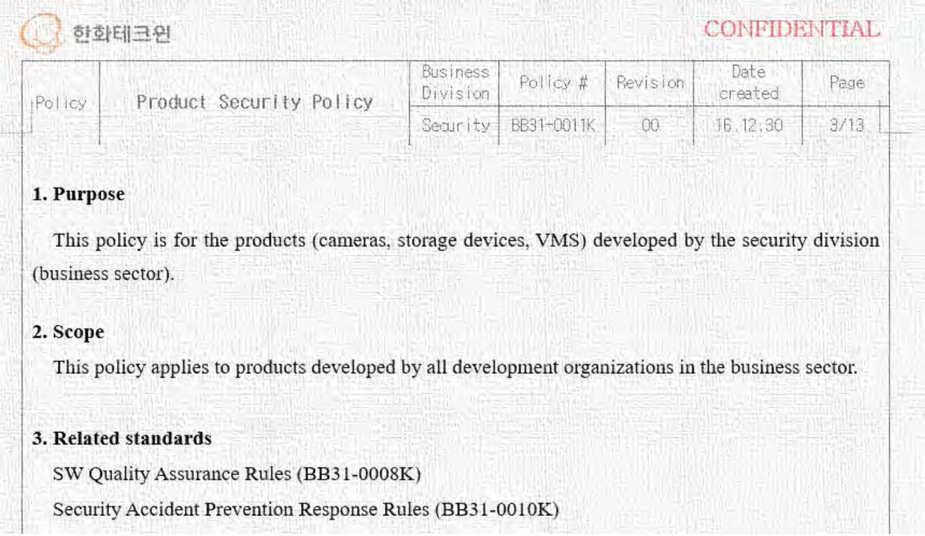
HACKERS LAB

Hanwha Techwin's leading security policy

The reason why we have been protected against hacking is that we recognized the importance of security and prepared in advance. From about 2 years ago, we have been conducting preliminary diagnosis of security vulnerabilities via an external agency to strengthen security of our security products. In January 2014, we used the S-CERT, Samsung SDS's Integrated Security Center to conduct the diagnosis on 5 security product families (NWC, HSS, NVR, DVR, and CMS) and in May 2016, we conducted a penetration test on network camera products via Hackers Lab, which is one of the leading companies in penetration test. Thus, we are constantly conducting activities to prevent security vulnerabilities and strengthen security of our products through security diagnosis and penetration test. We are also leading the security policy of our security solution products by thoroughly managing the product passwords which may have vulnerabilities as a result of user's carelessness.

Product Security Policy

Hanwha Techwin has developed and implemented a security policy that dictates the security design of products, including encryption/methods, password policy, firmware encryption, etc…



한화테크윈 CONFIDENTIAL

Policy	Product Security Policy	Business Division	Policy #	Revision	Date created	Page
		Security	BB31-0011K	00	16.12.30	3/13

1. Purpose

This policy is for the products (cameras, storage devices, VMS) developed by the security division (business sector).

2. Scope

This policy applies to products developed by all development organizations in the business sector.

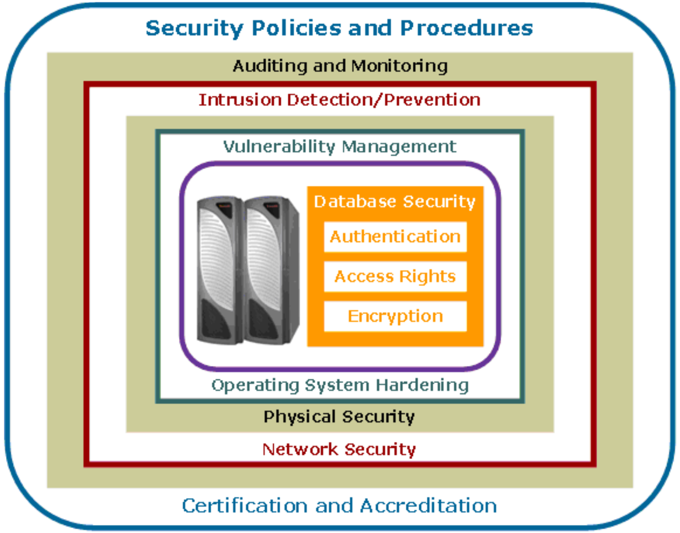
3. Related standards

SW Quality Assurance Rules (BB31-0008K)

Security Accident Prevention Response Rules (BB31-0010K)

Strategy

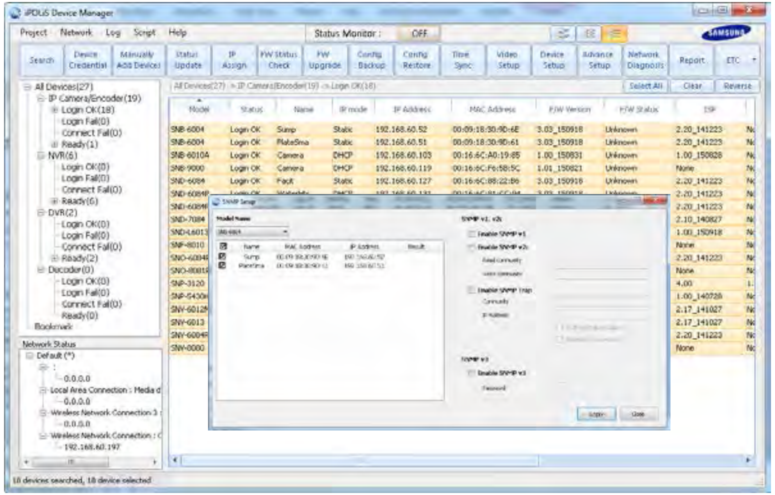
Using the **Defense in Depth** strategy for information system, it is important to have multiple layers of security. Do not rely on 1 features or mechanism as a safeguard.



Tools

When configuring Samsung network devices, it is recommended to use the WiseNet Device Manager for bulk operations.

https://www.hanwhasecurity.com/en/Tools/device-manager.aspx



All Devices(27)
- IP Camera/Encoder(19)
  - Login OK(18)
  - Login Fail(0)
  - Connect Fail(0)
  - Ready(1)
- NVR(6)
  - Login OK(0)
  - Login Fail(0)
  - Connect Fail(0)
  - Ready(6)
- DVR(2)
  - Login OK(0)
  - Login Fail(0)
  - Connect Fail(0)
  - Ready(2)
- Decoder(0)
  - Login OK(0)
  - Login Fail(0)
  - Connect Fail(0)
  - Ready(0)

Bookmark

Network Status
- Default (*)
  - :
    - 0.0.0.0
  - Local Area Connection : Media d
    - 0.0.0.0
  - Wireless Network Connection 3 :
    - 0.0.0.0
  - Wireless Network Connection : C
    - 192.168.60.197

All Devices(27) > IP Camera/Encoder(19) -> Login OK(18)

Model	Status	Name	IP mode	IP Address	MAC Address	F/W Version	F/W Status	ISP	
SNB-6004	Login OK	Sump	Static	192.168.60.52	00:09:18:30:9D:6E	3.03_150918	Unknown	2.20_141223	N
SNB-6004	Login OK	PlateSma	Static	192.168.60.51	00:09:18:30:9D:61	3.03_150918	Unknown	2.20_141223	N
SNB-6010A	Login OK	Camera	DHCP	192.168.60.103	00:16:6C:A0:19:85	1.00_150831	Unknown	1.00_150828	N
SNB-9000	Login OK	Camera	DHCP	192.168.60.119	00:16:6C:F6:58:5C	1.01_150821	Unknown	None	N
SND-6084	Login OK	Fact	Static	192.168.60.127	00:16:6C:88:22:B6	3.03_150918	Unknown	2.20_141223	N
SND-6084R	Login OK	[illegible]	DHCP	192.168.60.131	00:16:6C:81:CC:94	3.03_150918	Unknown	2.20_141223	N
SND-6084								2.20_141223	N
SND-7084								2.10_140827	N
SND-L6013								1.00_150918	N
SNF-8010								None	N
SNO-6084R								2.20_141223	N
SNO-8081R								None	N
SNP-3120								4.00	1.
SNP-5430H								1.00_140728	N
SNV-6012M								2.17_141027	N
SNV-6013								2.17_141027	N
SNV-6004R								2.20_141223	N
SNV-8000								None	N

SNMP Setup

Model Name: SNB-6004

☑	Name	MAC Address	IP Address	Result
☑	Sump	00:09:18:30:9D:6E	192.168.60.52	
☑	PlateSma	00:09:18:30:9D:61	192.168.60.51	

SNMP v1, v2c

☐ Enable SNMP v1

☐ Enable SNMP v2c

Read Community

Write Community

☐ Enable SNMP Trap

Community

IP Address

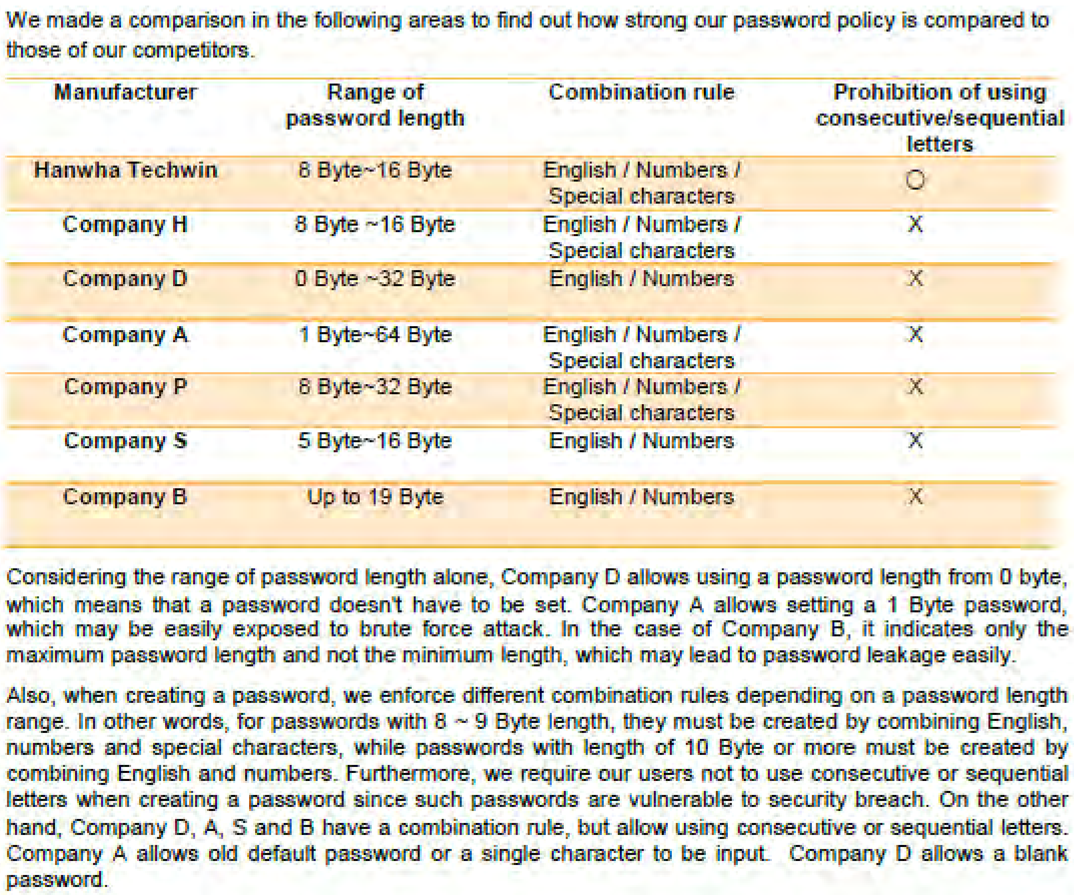
SNMP v3

☐ Enable SNMP v3

Password

18 devices searched, 18 device selected

Comparison of password policy strength



We made a comparison in the following areas to find out how strong our password policy is compared to those of our competitors.

Manufacturer	Range of password length	Combination rule	Prohibition of using consecutive/sequential letters
Hanwha Techwin	8 Byte~16 Byte	English / Numbers / Special characters	○
Company H	8 Byte ~16 Byte	English / Numbers / Special characters	X
Company D	0 Byte ~32 Byte	English / Numbers	X
Company A	1 Byte~64 Byte	English / Numbers / Special characters	X
Company P	8 Byte~32 Byte	English / Numbers / Special characters	X
Company S	5 Byte~16 Byte	English / Numbers	X
Company B	Up to 19 Byte	English / Numbers	X

Considering the range of password length alone, Company D allows using a password length from 0 byte, which means that a password doesn't have to be set. Company A allows setting a 1 Byte password, which may be easily exposed to brute force attack. In the case of Company B, it indicates only the maximum password length and not the minimum length, which may lead to password leakage easily.

Also, when creating a password, we enforce different combination rules depending on a password length range. In other words, for passwords with 8 ~ 9 Byte length, they must be created by combining English, numbers and special characters, while passwords with length of 10 Byte or more must be created by combining English and numbers. Furthermore, we require our users not to use consecutive or sequential letters when creating a password since such passwords are vulnerable to security breach. On the other hand, Company D, A, S and B have a combination rule, but allow using consecutive or sequential letters. Company A allows old default password or a single character to be input. Company D allows a blank password.

intel Security

HOW PASSWORD LENGTH WINS THE INTERNET

Passwords 102

Hanwha Techwin America

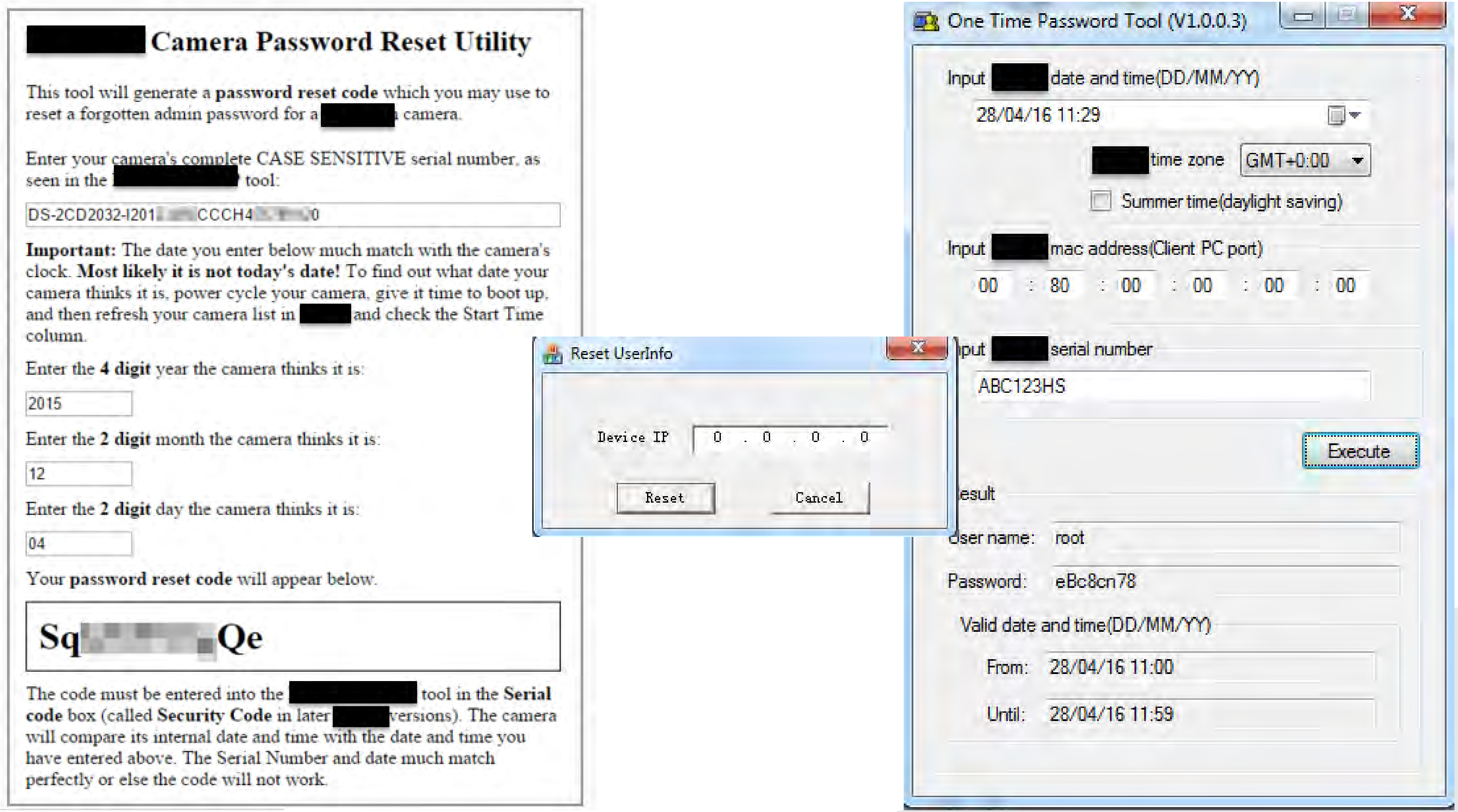
Backdoors?

A common request is how to gain access to a device in case the password is forgotten.   Many manufactures use a “one time use” password that combines the serial number/mac & the time/date.

Hanwha does not have any backdoor password/method for our devices.

This safeguards your device, requiring a factory default in case the password is lost.

Backdoors, cont.



[redacted] Camera Password Reset Utility

This tool will generate a **password reset code** which you may use to reset a forgotten admin password for a [redacted] camera.

Enter your camera's complete CASE SENSITIVE serial number, as seen in the [redacted] tool:

DS-2CD2032-I201[redacted]CCCH4[redacted]0

Important: The date you enter below much match with the camera's clock. **Most likely it is not today's date!** To find out what date your camera thinks it is, power cycle your camera, give it time to boot up, and then refresh your camera list in [redacted] and check the Start Time column.

Enter the **4 digit** year the camera thinks it is:

2015

Enter the **2 digit** month the camera thinks it is:

12

Enter the **2 digit** day the camera thinks it is:

04

Your **password reset code** will appear below.

Sq[redacted]Qe

The code must be entered into the [redacted] tool in the **Serial code** box (called **Security Code** in later [redacted] versions). The camera will compare its internal date and time with the date and time you have entered above. The Serial Number and date much match perfectly or else the code will not work.

Reset UserInfo

Device IP 0 . 0 . 0 . 0

One Time Password Tool (V1.0.0.3)

Input [redacted] date and time(DD/MM/YY)

28/04/16 11:29

[redacted] time zone GMT+0:00

□ Summer time(daylight saving)

Input [redacted] mac address(Client PC port)

00 : 80 : 00 : 00 : 00 : 00

put [redacted] serial number

ABC123HS

esult

ser name: root

Password: eBc8cn78

Valid date and time(DD/MM/YY)

From: 28/04/16 11:00

Until: 28/04/16 11:59

DoS attack/password guessing

If an incorrect username & password is given more than 5 times within 30 seconds, the camera will lock down access to the web page to prevent someone from repeatedly trying to guess the password. Existing authenticated video stream connections will continue.

All passwords are sent using digest authentication to prevent clear-text passwords from being transmitted over the network.

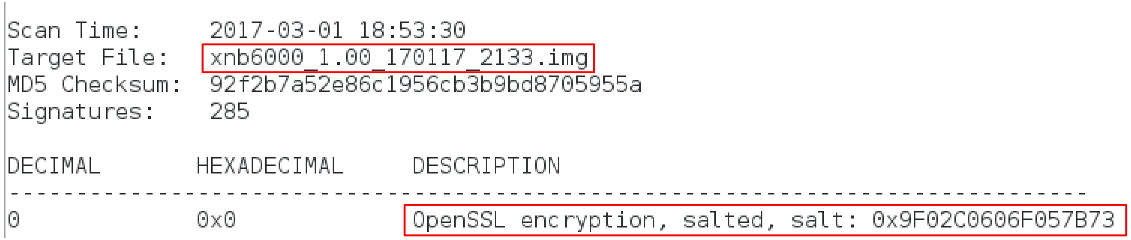
Buffer overflow, unused ports

All commands are filtered by our own source code and passed to the web server after a validation check to prevent hacking and overflows. This protects from “injection” attacks which try to bypass authentication, or overflowing services to allowing access.

Unused services and ports are disabled in the Linux to prevent access to telnet, FTP, SSH, shell, etc. to prevent overflow, hacking, etc., as they are not used/needed.

Safe firmware upgrades

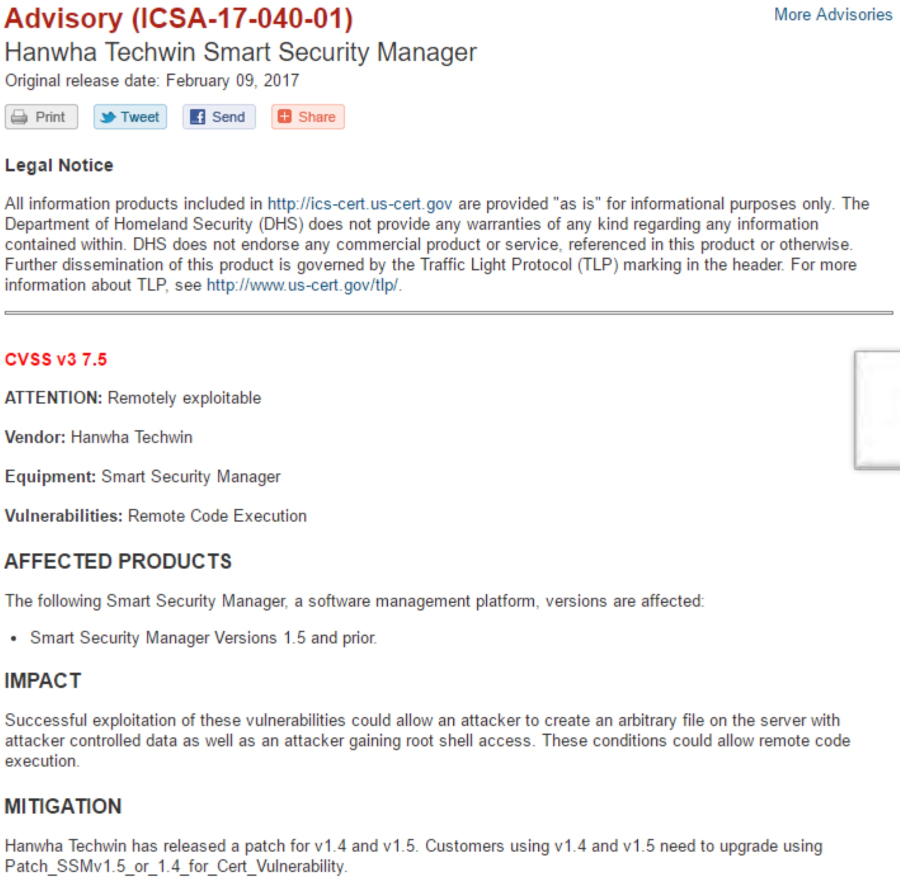
- Make sure firmware and VMS software is up to date to ensure any fixes or new daemon software is used, in case of any known vulnerabilities.
- Firmware can be checked, downloaded & updated in bulk, both online or offline using Device Manager.
- Include firmware updates as part of your installation service (initial, 6 months, 1year out), then as RMR.
- Firmware files should be encrypted to prevent hackers from gaining valuable info about file structure, files, databases, etc. Often hackers can discover a vulnerability simply by examining extracted firmware without access to the device.



```
Scan Time:      2017-03-01 18:53:30
Target File:    xnb6000_1.00_170117_2133.img
MD5 Checksum:   92f2b7a52e86c1956cb3b9bd8705955a
Signatures:     285

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             OpenSSL encryption, salted, salt: 0x9F02C0606F057B73
```

A vulnerability was reported with SSM. A patch was quickly released for versions 1.4/1.5. Version 1.6 does not need the patch



Advisory (ICSA-17-040-01)

Hanwha Techwin Smart Security Manager

Original release date: February 09, 2017

Legal Notice

All information products included in http://ics-cert.us-cert.gov are provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. DHS does not endorse any commercial product or service, referenced in this product or otherwise. Further dissemination of this product is governed by the Traffic Light Protocol (TLP) marking in the header. For more information about TLP, see http://www.us-cert.gov/tlp/.

CVSS v3 7.5

ATTENTION: Remotely exploitable

Vendor: Hanwha Techwin

Equipment: Smart Security Manager

Vulnerabilities: Remote Code Execution

AFFECTED PRODUCTS

The following Smart Security Manager, a software management platform, versions are affected:

- Smart Security Manager Versions 1.5 and prior.

IMPACT

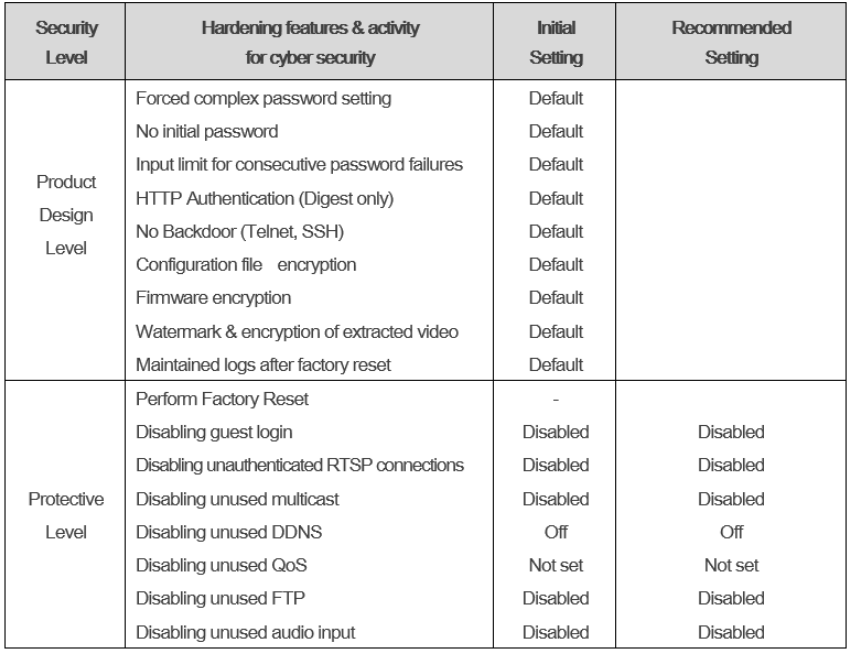
Successful exploitation of these vulnerabilities could allow an attacker to create an arbitrary file on the server with attacker controlled data as well as an attacker gaining root shell access. These conditions could allow remote code execution.

MITIGATION

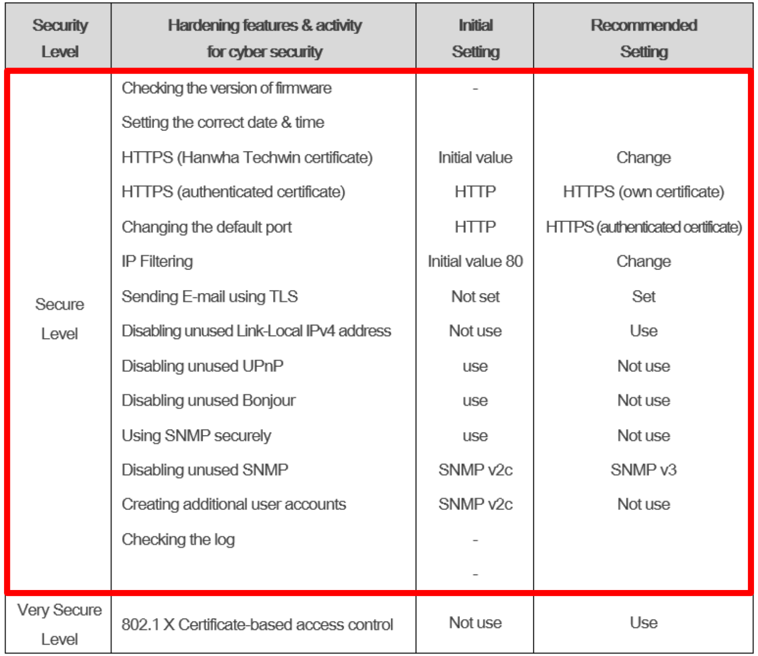
Hanwha Techwin has released a patch for v1.4 and v1.5. Customers using v1.4 and v1.5 need to upgrade using Patch_SSMv1.5_or_1.4_for_Cert_Vulnerability.

No known public exploits specifically target these vulnerabilities

Best Practices as per Hardening Guide



Security Level	Hardening features & activity for cyber security	Initial Setting	Recommended Setting
Product Design Level	Forced complex password setting	Default	
	No initial password	Default	
	Input limit for consecutive password failures	Default	
	HTTP Authentication (Digest only)	Default	
	No Backdoor (Telnet, SSH)	Default	
	Configuration file encryption	Default	
	Firmware encryption	Default	
	Watermark & encryption of extracted video	Default	
	Maintained logs after factory reset	Default	
Protective Level	Perform Factory Reset	-	
	Disabling guest login	Disabled	Disabled
	Disabling unauthenticated RTSP connections	Disabled	Disabled
	Disabling unused multicast	Disabled	Disabled
	Disabling unused DDNS	Off	Off
	Disabling unused QoS	Not set	Not set
	Disabling unused FTP	Disabled	Disabled
	Disabling unused audio input	Disabled	Disabled

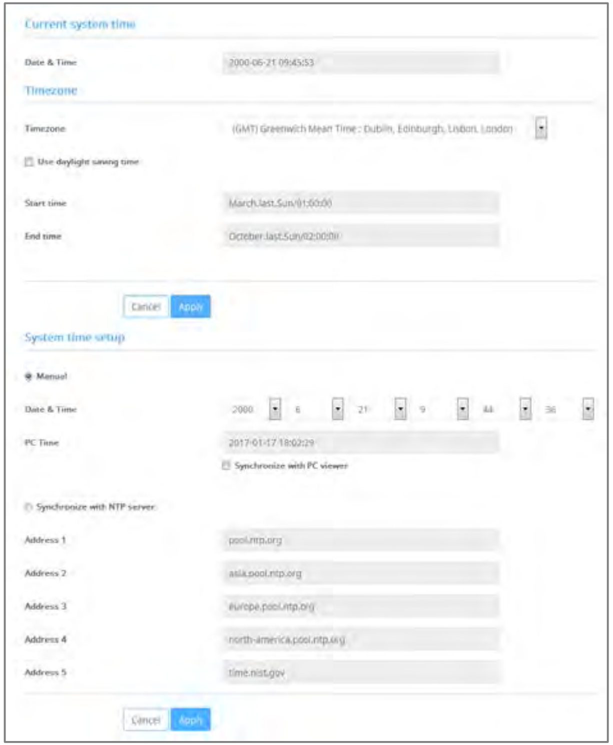


Security Level	Hardening features & activity for cyber security	Initial Setting	Recommended Setting
Secure Level	Checking the version of firmware	-	
	Setting the correct date & time		
	HTTPS (Hanwha Techwin certificate)	Initial value	Change
	HTTPS (authenticated certificate)	HTTP	HTTPS (own certificate)
	Changing the default port	HTTP	HTTPS (authenticated certificate)
	IP Filtering	Initial value 80	Change
	Sending E-mail using TLS	Not set	Set
	Disabling unused Link-Local IPv4 address	Not use	Use
	Disabling unused UPnP	use	Not use
	Disabling unused Bonjour	use	Not use
	Using SNMP securely	use	Not use
	Disabling unused SNMP	SNMP v2c	SNMP v3
	Creating additional user accounts	SNMP v2c	Not use
	Checking the log	-	
		-	
Very Secure Level	802.1 X Certificate-based access control	Not use	Use

Hanwha Techwin America

Time & Date

- The built in clock keeps the date and time up to date. It is important to check that the clock is correct when deploying a device. The clock is used to record logs and for recording video. If the clock is incorrect, forensic investigation in case of a network breach will be very difficult. Furthermore, the video evidence may not be admissible in court if the clock is not accurate. Finally, many other services rely on an accurate clock and may fail to work properly if the clock is not set correctly, including HTTPS, ONVIF, SNMP v3, and 802.1x.
- The NTP protocol can be used to ensure that over time the clock does not drift and stays accurate. All Hanwha Techwin NVRs feature an NTP server for cameras to sync to when enabled.



Current system time

Date & Time: 2000-06-21 09:45:53

Timezone

Timezone: (GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London

□ Use daylight saving time

Start time: March.last.Sun/01:00:00

End time: October.last.Sun/02:00:00

System time setup

● Manual

Date & Time: 2000 / 6 / 21 / 9 / 44 / 36

PC Time: 2017-01-17 18:02:29

□ Synchronize with PC viewer

○ Synchronize with NTP server

Address 1: pool.ntp.org

Address 2: asia.pool.ntp.org

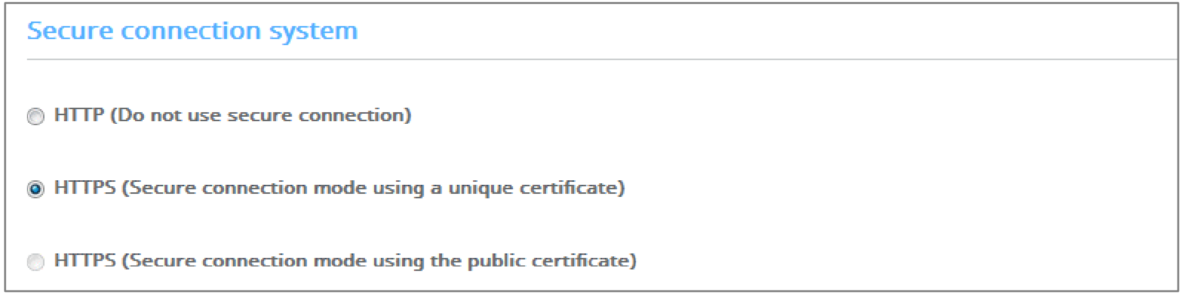
Address 3: europe.pool.ntp.org

Address 4: north-america.pool.ntp.org

Address 5: time.nist.gov

HTTPS Mode

- HTTPS (Hanwha Techwin certificate) is a function that enables a secure connection between the device and client using a certificate provided by Hanwha Techwin. If you select 'HTTPS (Secure connection mode using a unique certificate)', the device's built-in certificate will be used in secure connection mode and you do not need to purchase and install a separate certificate. Once enabled, communications will occur over the HTTPS port. HTTPS also helps ensure the communications are not intercepted/redirected.



Secure connection system

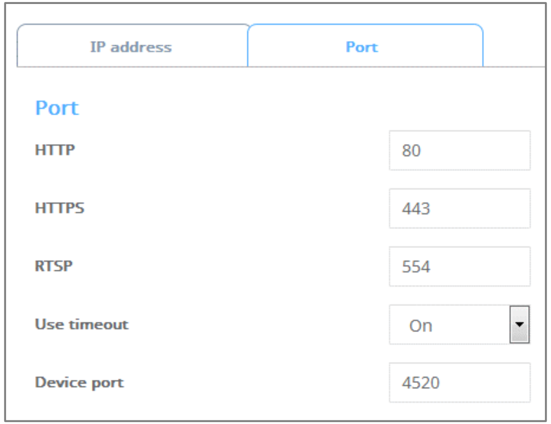
○ HTTP (Do not use secure connection)

● HTTPS (Secure connection mode using a unique certificate)

○ HTTPS (Secure connection mode using the public certificate)

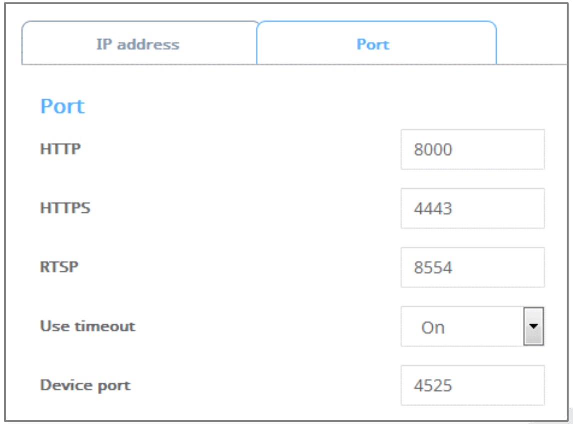
Changing the default ports

- In order to better avoid scans or attacks through the well-known default port of a network device, it is recommended to change the port. Commonly higher port numbers will be used, such as 8000+ or 10000+. For example, if you change the HTTP web service port to 8000 rather than 80, you can protect your web server from attacks from simple scanning programs or attempt to enter addresses directly into a web browser.
- For example, prevent a hacker from quickly scanning for port 4520 to try to find Hanwha devices.



Port

HTTP	80
HTTPS	443
RTSP	554
Use timeout	On
Device port	4520

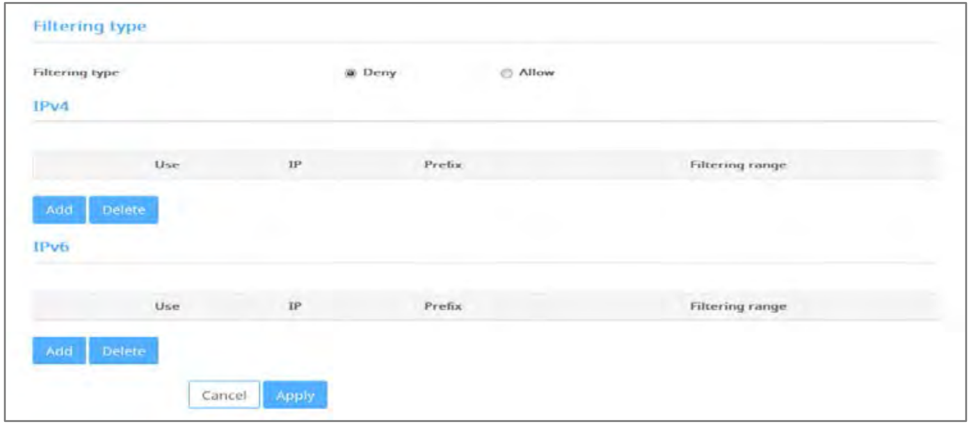


Port

HTTP	8000
HTTPS	4443
RTSP	8554
Use timeout	On
Device port	4525

IP Filtering

- Hanwha Techwin products support the creation of IP lists to allow or deny access from specific IP address. This can be used to restrict access only to the security department, or to prevent access from the WAN router or wireless pool of IP addresses.
- Menu prevents lockout of admin PC.



Filtering type

Filtering type ● Deny ○ Allow

IPv4

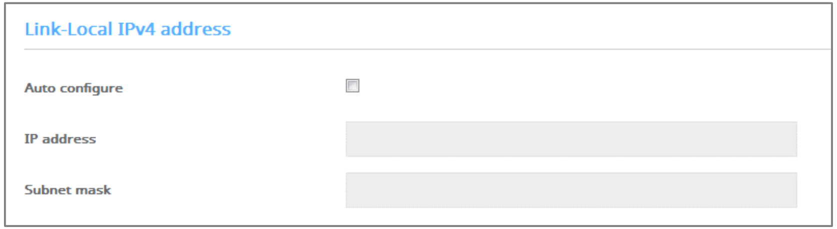
Use	IP	Prefix	Filtering range

IPv6

Use	IP	Prefix	Filtering range

Disable unused protocols:

- Disable unused Link-Local IPv4 address
- Disable unused UPnP
- Disable unused Bonjour

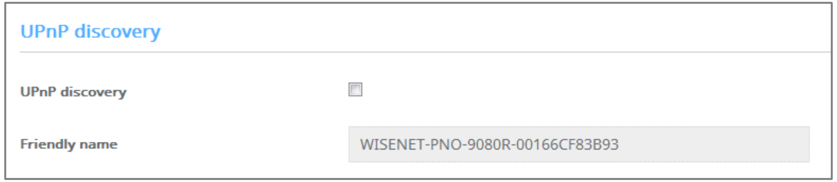


Link-Local IPv4 address

Auto configure ☐

IP address

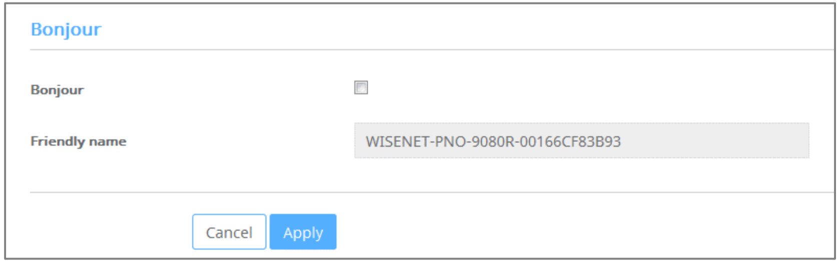
Subnet mask



UPnP discovery

UPnP discovery ☐

Friendly name WISENET-PNO-9080R-00166CF83B93



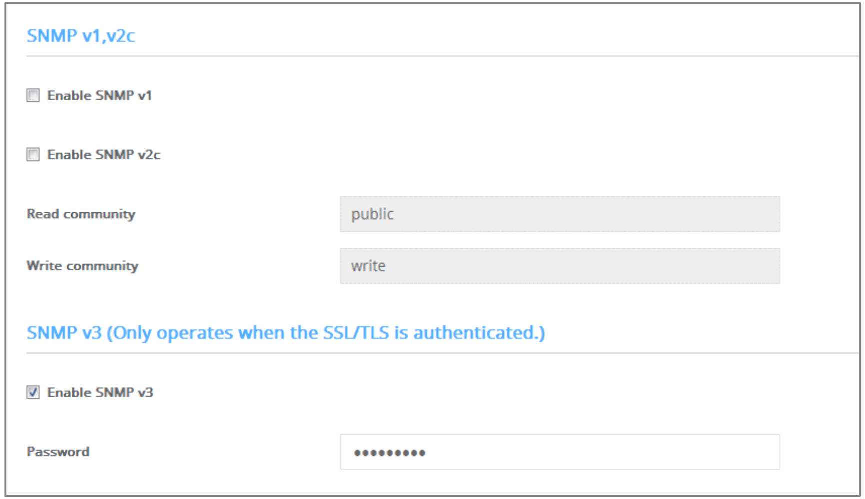
Bonjour

Bonjour ☐

Friendly name WISENET-PNO-9080R-00166CF83B93

Using SNMP securely or disabled

- SNMP provides the ability to conveniently manage network devices. However, SNMP v1 and v2c are vulnerable because they use clear text strings. If you want to use this function, it is recommended to use the secure SNMP v3 only. SNMP v3 is only available when the camera is running in HTTPS mode.



SNMP v1,v2c

□ Enable SNMP v1

□ Enable SNMP v2c

Read community: public

Write community: write

SNMP v3 (Only operates when the SSL/TLS is authenticated.)

☑ Enable SNMP v3

Password: ●●●●●●●●●●

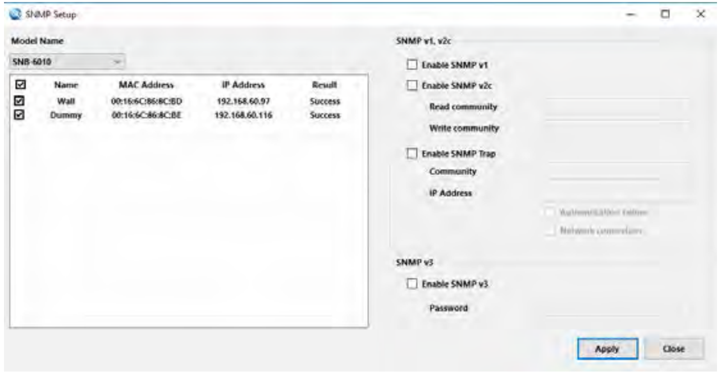
Disabling SNMP

- Wisenet X series allows SNMP to be disabled via the web viewer. Other models require using the Wisenet Device Manager or CGI commands to disable all SNMP versions.
  - Disable SNMP v2c

http://(ip address)/stw-cgi/network.cgi?msubmenu=snmp&action=set&Version2=False

  - Disable SNMP v1

http://(ip address)/stw-cgi/network.cgi?msubmenu=snmp&action=set&Version1=False



Model Name

SNB-6010

☑	Name	MAC Address	IP Address	Result
☑	Wall	00:16:6C:86:8C:BD	192.168.60.97	Success
☑	Dummy	00:16:6C:86:8C:BE	192.168.60.116	Success

SNMP v1, v2c

□ Enable SNMP v1

□ Enable SNMP v2c

Read community

Write community

□ Enable SNMP Trap

Community

IP Address

□ Authentication failure

□ Network connection

SNMP v3

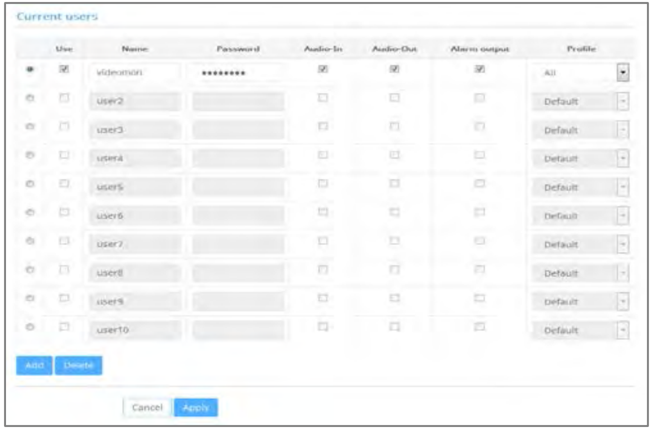
□ Enable SNMP v3

Password

*This should be addressed in future firmware updates.

Create user-level accounts for daily use

- Accessing the device only with an administrator account can cause the administrator password to be continuously transmitted over the network, which can lead to a security vulnerability that exposes sensitive information to a person who has malicious purposes. Furthermore, users then have escalated privileges, whereas they should only have the least required privileges to perform their job functions to prevent accidental or malicious settings changes.
- Therefore, you can enhance your security by using the administrator account for configuration only, and adding user accounts with limited privileges, such as frequently used video monitoring features.



Current users

	Use	Name	Password	Audio-In	Audio-Out	Alarm output	Profile
●	☑	videomon	********	☑	☑	☑	All
○	□	user2		□	□	□	Default
○	□	user3		□	□	□	Default
○	□	user4		□	□	□	Default
○	□	user5		□	□	□	Default
○	□	user6		□	□	□	Default
○	□	user7		□	□	□	Default
○	□	user8		□	□	□	Default
○	□	user9		□	□	□	Default
○	□	user10		□	□	□	Default

802.1x Port-based Network Access Control

802.1x is used in cases where network jacks are accessible in public areas, or in unmonitored areas where someone could unplug a device and plug in their own laptop, etc.

In an 802.1x network environment, the network switch will only talk to specific devices.

In conventional schemes, you would use IP address or MAC address filtering, but these can be easily circumvented.

All 802.1x devices have a certificate generated and installed to positively identify them.

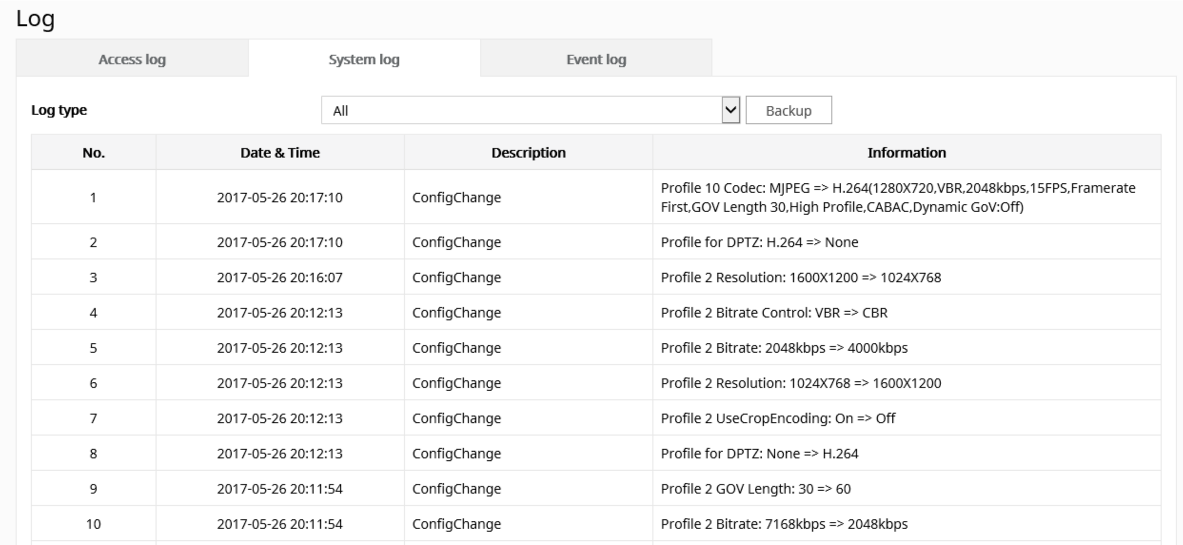
A RADIUS Server is used to authenticate devices.

Check device logs

Samsung products have extensive logs. Check them to see if anyone is trying to gain access to your devices or has changed settings.

Logs are retained during reboot and factory default.

Logs show current and new configuration change values.



Log type: All

No.	Date & Time	Description	Information
1	2017-05-26 20:17:10	ConfigChange	Profile 10 Codec: MJPEG => H.264(1280X720,VBR,2048kbps,15FPS,Framerate First,GOV Length 30,High Profile,CABAC,Dynamic GoV:Off)
2	2017-05-26 20:17:10	ConfigChange	Profile for DPTZ: H.264 => None
3	2017-05-26 20:16:07	ConfigChange	Profile 2 Resolution: 1600X1200 => 1024X768
4	2017-05-26 20:12:13	ConfigChange	Profile 2 Bitrate Control: VBR => CBR
5	2017-05-26 20:12:13	ConfigChange	Profile 2 Bitrate: 2048kbps => 4000kbps
6	2017-05-26 20:12:13	ConfigChange	Profile 2 Resolution: 1024X768 => 1600X1200
7	2017-05-26 20:12:13	ConfigChange	Profile 2 UseCropEncoding: On => Off
8	2017-05-26 20:12:13	ConfigChange	Profile for DPTZ: None => H.264
9	2017-05-26 20:11:54	ConfigChange	Profile 2 GOV Length: 30 => 60
10	2017-05-26 20:11:54	ConfigChange	Profile 2 Bitrate: 7168kbps => 2048kbps

VLANs

VLANs segregate your network based upon ports, protocols, MAC addresses, port switches, etc.

This isolates your cameras from your printers, e-mail servers, workstations, etc., and only gives access to those who need access.

This can also prevent problems from devices broadcasting or babbling and effecting other devices.

Physical Access

Physical Access is paramount. If you can touch a camera, you can factory default it, and then do what you want with it.

It is best if your cameras are high up, out of reach, or flush mounted in the ceiling or a housing.

Make sure your NVRs and switches are in a locked area.

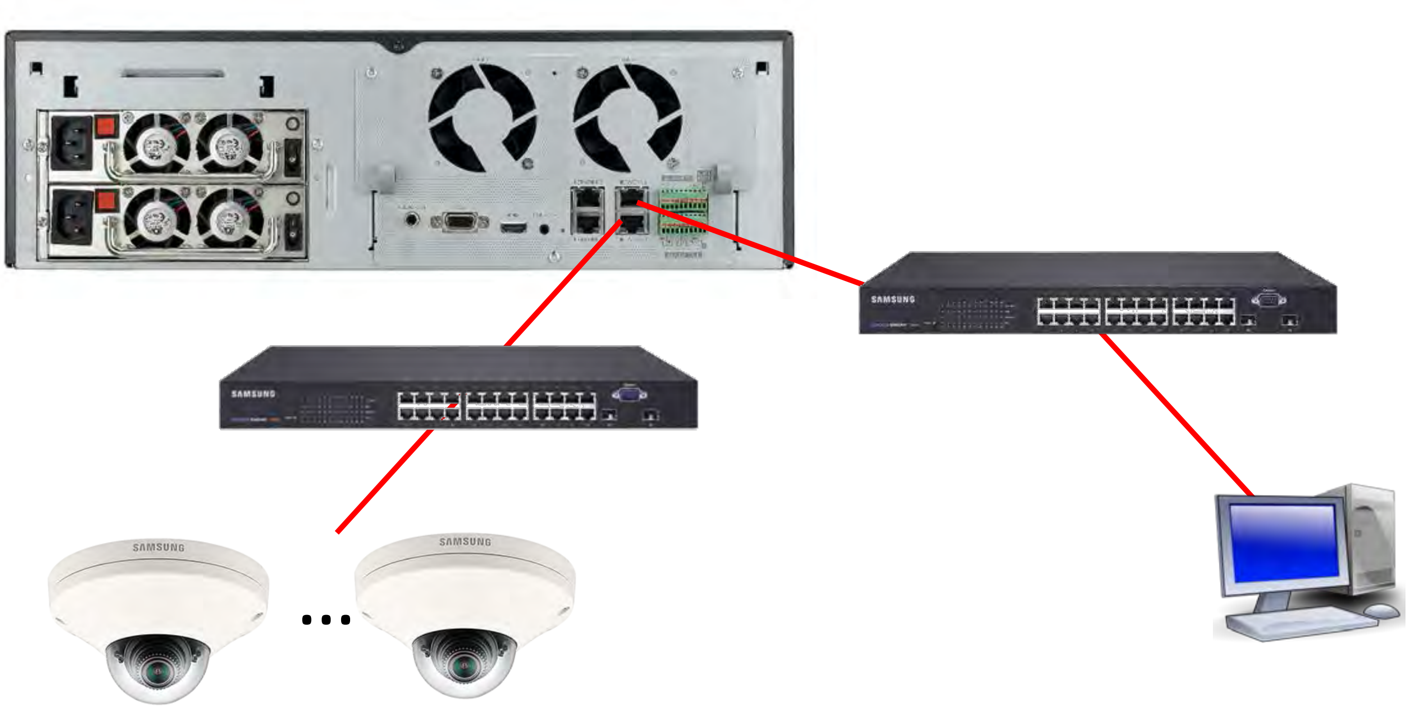
Make sure the network and power cables going to cameras are secure. If someone can reach up and cut them, it is not secure.

Physical Access - 2

Make a backup of the device programming, in case you need to factory default it.

Have some recognizable settings so you can identify if someone has defaulted your device (SNMP settings can be great here).

Example - No direct access to camera



Open Platform Apps

- Open Platform Apps are sandboxed – they are NOT allowed root access to the camera/file system. This protects the camera from malicious access.
- Other manufacturer implementations allow direct root access to camera file system to 3rd party apps.

Remote access

- Use VPNs when possible for encrypted remote access without opening holes in the firewall.
- When you provide remote access, use port forwarding, and not UPnP.
- Only forward necessary ports, such as to the NVR as opposed to ***each camera***.
- If you are using another mechanism for remote access, such as VPN, do not forward the cameras through the router/firewall.
- P2P can be used to provide remote access without opening firewall. Some enterprises will not want P2P punching out. In this case, disable P2P function.

Thank You!
http://www.hanwhasecurity.com

Hanwha
Techwin America