Securing Video Surveillance Devices to Close Network Vulnerabilities
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: 08/20/2016
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 absctmsgXtb3o:0:0:root:/bin/sh
/etc $ cat passwd
root absctmsgXtb3o: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 XiongMai 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:~$ /usr/pkg/General_General_AHB7804R-MH-V2_V4.02.R117601.20160924.bin.extracted/_romfs-x.cramfs.img.extracted/squashfs-root/etc# cat passwd
root absctmsgXtb3o:0:0:root:/bin/sh
root@localhost:~$ /usr/pkg/General_General_AHB7804R-MH-V2_V4.02.R117601.20160924.bin.extracted/_romfs-x.cramfs.img.extracted/squashfs-root/etc# cat init.d/rcS 1 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-2016-1000245
Reporter: Flashpoint
Discover Date: 09/29/2016
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 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.
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 Venmulapalli, 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 Venmulapalli, 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 Venmulapalli.

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,” Venmulapalli 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 (ICS-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:
- CCMV3025: All versions prior to 1.41_SP18_S1,
- CMAV3025-R: All versions prior to 1.41_SP18_S1,
- CFMV3025: All versions prior to 1.41_SP18_S1,
- CCPE3025: All versions prior to 0.1.73_S1,
- CCPEV5025: All versions prior to 0.1.73_S1,
- CCMD3025-DN10: All versions prior to v1.394_S1,
- CCID1445-DN18: All versions prior to v2635,
- COD1446-DN28: All versions prior to v2635,
- COD1445-DN38: All versions prior to v2635,
- CF1S1425: All versions prior to v2635,
- COC11425: All versions prior to v2635,
- CFMS2025: All versions prior to v2635,
- CCMW2026: All versions prior to v2635,
- CMMA2025-R: All versions prior to v2635,
- CMMAV1025: 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.
Vulnerability Note VU#856152
NUUO and Netgear Network Video Recorder (NVR) products web interfaces contain multiple vulnerabilities

Overview
NUUO NVRmini 2, NVRails, 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, NVRails, 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 also be vulnerable if they use the same web interface; firmware versions earlier than those specified below may also be vulnerable.

CWE-28: Improper Input Validation - CVE-2016-6674
The web management interfaces of affected devices contain a hidden page, __debugging_center_utilis.php, that fails to properly validate the $param 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_utilis.php?log=something%0B%0apayload>

CWE-2018-6674 has been confirmed by the researcher to affect the NUUO NVRmini 2 and NVRails, versions 1.7.6 to 3.6.0, and the ReadyNAS Surveillance, both x86 and ARM, versions 1.1.1 to 1.4.1. The CVSS score below describes CWE-2018-6674.

CWE-28: Improper Input Validation - CVE-2016-6676
The handle_daylightsaving.php page does not sanitize the $servername 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=updateHTTPServer=something%0B%0apayload>

CWE-2016-6675 has been confirmed by the researcher to affect:
- NUUO NVRmini 2, versions 1.7.5 to 3.0.0
- NUUO NVRails, versions 1.0.9 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. For example, an unauthenticated attacker can make a request for:
http://[IP]/cgi-bin/cgi_system&load=stdout

CWE-2016-5676 has been confirmed by the researcher to affect NUUO NVRmini 2 and NVRails versions 1.7.5 to 3.6.0, versions 2.2.1 and 3.8.8 require authentication, and ReadyNAS Surveillance, both x86 and ARM, versions 1.1.1 to 1.4.1.

CWE-208: Information Exposure - CVE-2016-6677
CWE-2018-6677 has been confirmed by the researcher to affect:
- NUUO NVRmini 2, versions 1.7.5 to 3.0.0
- NUUO NVRails, versions 1.0.6 to 3.0.0
- ReadyNAS Surveillance, both x86 and ARM versions 1.1.1 to 1.4.1

According to the researcher, NUUO NVRmini 2 and NVRails 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-77: Improper Neutralization of Special Elements used in an OS Command (OS Command Injection) - CVE-2015-5679
The $_file parameter of the transfer_license command in cgi_main does not properly validate unprovided input. An authenticated attacker may make a specially crafted request to execute arbitrary commands:
http://[IP]/cgi-bin/cgi_main?handler=transfer_license&method=offLine&error庑ommand=#

CWE-77 has been confirmed by the researcher to affect NUUO NVRmini 2 versions 1.7.5 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-2016-6680
The $name 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?handler=transfer_license&method=offLine&error廯payload>

CWE-2016-6680 can be exploited by any user locally, but requires an administrator account for remote exploitation.
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-4010 NVR firmware prior to v2.36_1F3401.zip
Hanwha SRN-3670587758/42758 NVR firmware prior to v3.08_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 administrative 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 device.

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-45725: (Products > Video Recorders > SRN-45725 > Download > Firmware)
SRN-45735: (Products > Video Recorders > SRN-45735 > Download > Firmware)
SRN-45738: (Products > Video Recorders > SRN-45738 > Download > Firmware)
What is Hanwha Techwin doing to keep your systems safe and secure??
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, many of the most high-profile data breaches that have occurred recently have been 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, IP personnel, and System Integrators installing systems to determine the level of security needed while balancing the cost 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).

Summary

The harsh reality in today’s connected world is that individuals and groups will continue their attempts to identify and exploit weaknesses in your network security. And while we should appreciate the convenience of a growing number of devices available to them, the reality is that these devices only increase the likelihood of unauthorized network access. Therefore, it is vital that all off-these-devices are taken into account when designing an ‘air-tight’ network for hackers. Implementing these best practices not only can prevent unauthorized access and systems from going in entry points, but it will ensure the security and continued operation of all critical functions, including the ability to monitor safety and security at a place and event. 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.

Personally, 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, I.T. department, the installer, and systems integrator are the key to finding the best solution to fit an individual organization’s security needs.
2. Definition of Security Levels

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 in the states immediately after the factory initialization.
- The secure level is a level of security that users 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 Levels

<table>
<thead>
<tr>
<th>Security Level</th>
<th>Hardening features &amp; activity for cyber security</th>
<th>Initial Setting</th>
<th>Recommended Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product Design Level</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Format complex password setting</td>
<td>Default</td>
<td>Default</td>
</tr>
<tr>
<td></td>
<td>No Telnet</td>
<td>Default</td>
<td>Default</td>
</tr>
<tr>
<td></td>
<td>HTTP Authentication (HTTPS only)</td>
<td>Default</td>
<td>Default</td>
</tr>
<tr>
<td></td>
<td>No DDOS Detection (DDoS)</td>
<td>Default</td>
<td>Default</td>
</tr>
<tr>
<td></td>
<td>Configuration &amp; encryption</td>
<td>Default</td>
<td>Default</td>
</tr>
<tr>
<td></td>
<td>Firmware encryption</td>
<td>Default</td>
<td>Default</td>
</tr>
<tr>
<td></td>
<td>Watermark &amp; encryption of unlinked video</td>
<td>Default</td>
<td>Default</td>
</tr>
<tr>
<td></td>
<td>Watermark after factory reset</td>
<td>Default</td>
<td>Default</td>
</tr>
<tr>
<td>Protective Level</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Performance/Reset</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td></td>
<td>Disabled guest login</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td></td>
<td>Disabling unprivileged &amp; un的身份</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td></td>
<td>Disabling unauthorized HTTPS connections</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td></td>
<td>Disabling unauthorized TFTP connections</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td></td>
<td>Disabling unauthorized PTP</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td></td>
<td>Disabling unauthorized QoS</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td></td>
<td>Disabling unauthorized PTP</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td></td>
<td>Disabling unauthorized multi-protocol</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

*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 – 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

Improvement of vulnerabilities that reported from various organization (since 2012)
Cookies, User authentication, Backdoor, Firmware & video encryption, etc.
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...

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

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.

<table>
<thead>
<tr>
<th>Manufacturer</th>
<th>Range of password length</th>
<th>Combination rule</th>
<th>Prohibition of using consecutive/sequential letters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hanwha Techwin</td>
<td>8 Byte~16 Byte</td>
<td>English / Numbers / Special characters</td>
<td>○</td>
</tr>
<tr>
<td>Company H</td>
<td>8 Byte~16 Byte</td>
<td>English / Numbers / Special characters</td>
<td>×</td>
</tr>
<tr>
<td>Company D</td>
<td>0 Byte~32 Byte</td>
<td>English / Numbers</td>
<td>×</td>
</tr>
<tr>
<td>Company A</td>
<td>1 Byte~64 Byte</td>
<td>English / Numbers / Special characters</td>
<td>×</td>
</tr>
<tr>
<td>Company P</td>
<td>8 Byte~32 Byte</td>
<td>English / Numbers / Special characters</td>
<td>×</td>
</tr>
<tr>
<td>Company S</td>
<td>5 Byte~16 Byte</td>
<td>English / Numbers</td>
<td>×</td>
</tr>
<tr>
<td>Company B</td>
<td>Up to 19 Byte</td>
<td>English / Numbers</td>
<td>×</td>
</tr>
</tbody>
</table>

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.

HOW PASSWORD LENGTH WINS THE INTERNET Passwords 102
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.

Camera Password Reset Utility
This tool will generate a password reset code which you may use to reset a forgotten admin password for a camera.

Enter your camera's complete CASE SENSITIVE serial number, as seen in the tool:
DS-2CD2032-I201

Important: The date you enter below must 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 the tool 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\_Qe

The code must be entered into the tool in the Serial code box (called Security Code in later versions). The camera will compare its internal date and time with the date and time you have entered above. The Serial Number and date must match perfectly or else the code will not work.
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.
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_SSM_v1.5_or_1.4_for_Cert_Vulnerability.
## Best Practices as per Hardening Guide

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

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

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

*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.
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.

<table>
<thead>
<tr>
<th>No.</th>
<th>Date &amp; Time</th>
<th>Description</th>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2017-05-26 20:17:10</td>
<td>ConfigChange</td>
<td>Profile 10 Codec: MPEG =&gt; H.264[1280x720,VBR,2048kbps,15FPS,Framerate First,GOV Length 30,High Profile,CABAC,Dynamic GoC Off]</td>
</tr>
<tr>
<td>2</td>
<td>2017-05-26 20:17:10</td>
<td>ConfigChange</td>
<td>Profile for DPTZ: H.264 =&gt; None</td>
</tr>
<tr>
<td>3</td>
<td>2017-05-26 20:16:07</td>
<td>ConfigChange</td>
<td>Profile 2 Resolution: 1600X1200 =&gt; 1024X768</td>
</tr>
<tr>
<td>4</td>
<td>2017-05-26 20:12:13</td>
<td>ConfigChange</td>
<td>Profile 2 Bitrate Control: VBR =&gt; CBR</td>
</tr>
<tr>
<td>5</td>
<td>2017-05-26 20:12:13</td>
<td>ConfigChange</td>
<td>Profile 2 Bitrate: 2048kbps =&gt; 4000kbps</td>
</tr>
<tr>
<td>6</td>
<td>2017-05-26 20:12:13</td>
<td>ConfigChange</td>
<td>Profile 2 Resolution: 1024X768 =&gt; 1600X1200</td>
</tr>
<tr>
<td>7</td>
<td>2017-05-26 20:12:13</td>
<td>ConfigChange</td>
<td>Profile 2 UseCropEncoding: On =&gt; Off</td>
</tr>
<tr>
<td>8</td>
<td>2017-05-26 20:12:13</td>
<td>ConfigChange</td>
<td>Profile for DPTZ: None =&gt; H.264</td>
</tr>
<tr>
<td>9</td>
<td>2017-05-26 20:11:54</td>
<td>ConfigChange</td>
<td>Profile 2 GOV Length: 30 =&gt; 60</td>
</tr>
<tr>
<td>10</td>
<td>2017-05-26 20:11:54</td>
<td>ConfigChange</td>
<td>Profile 2 Bitrate: 7168kbps =&gt; 2048kbps</td>
</tr>
</tbody>
</table>
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