Hanwha Techwin

White Paper

Guidelines for secure use of ONVIF WS-Discovery

22 09, 2020

Contents

Revision history

Version	Date	Content	Remarks
v1.0	20200922	Initial creation	

1. Occurrence of denial of service attacks

Denial-of-service (DoS) attacks using the ONVIF WS-Discovery service were recently launched against our cameras exposed to a public network. The attacks did not affect cameras installed on internal or local networks. Cameras that are connected to a public network where the ONVIF WS-Discovery service is disabled were not affected by the attack.

Users should take precautions even if they have no intention to use the service as ONVIF WS-Discovery is activated by default for user convenience and attackers can abuse the service to launch DoS campaigns.

Against this backdrop, Hanwha Techwin is distributing this "Guidelines for secure use of ONVIF WS-Discovery" to help users better understand and utilize the security features of the WS-Discovery service in our products.

2. Secure use of WS-Discovery

2.1. Introduction of "WS-Discovery"

Web Service Dynamic Discovery (WS-Discovery) is a multicast discovery protocol used for locating devices or services on a network. Devices such as NVRs or a VMS utilize WS-Discovery to search and connect to cameras, making the service essential in an ONVIF environment.

Our devices support the Device Discovery service based on the ONVIF WS-Discovery protocol.

2.2. Disable WS-Discovery on a public network

Although WS-Discovery offers convenience in managing camera devices, it can also allow cyberattacks such as DoS attacks. Camera devices open to a wide area network (WAN) are more vulnerable to DoS attacks.

Hanwha Techwin recommends to disable ONVIF WS-Discovery on cameras operating on a WAN. If cameras are open to a WAN, users should apply the following security settings as a precaution. Additional safeguards can be taken such as placing the camera behind a router with Network Address Translation and blocking unnecessary ports and services. The use of a router can prevent this type of attack from occurring by limiting external access to the camera, and can eliminate the need to disable the ONVIF WS-Discovery protocol.

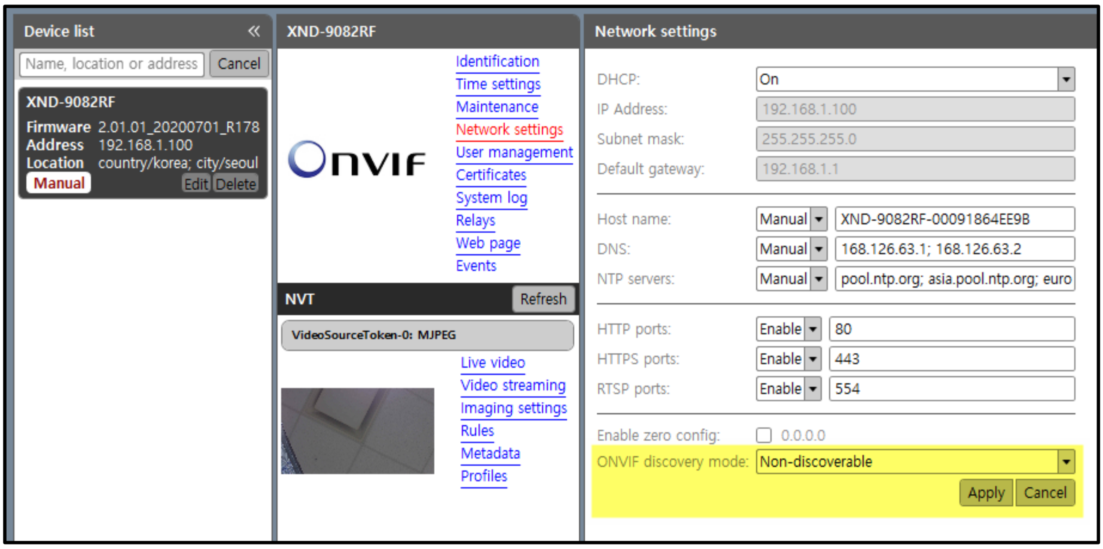
[Disable ONVIF WS-Discovery in settings]

1) Download the 3rd party, free ONVIF Device manager from https://sourceforge.net/projects/onvifdm/. Use ONVIF Device Manager to search for cameras on the network

2) Enter the ID / password to connect to the cameras

3) Menu: Network setting → Select "Non-discoverable" in ONVIF discovery mode and apply

   Note) NVRs or VMS may no longer discover a device for device management. You may need to manually enroll devices.



XND-9082RF
Firmware 2.01.01_20200701_R178
Address 192.168.1.100
Location country/korea; city/seoul
Manual

DHCP:	On	
IP Address:	192.168.1.100	
Subnet mask:	255.255.255.0	
Default gateway:	192.168.1.1	
Host name:	Manual	XND-9082RF-00091864EE9B
DNS:	Manual	168.126.63.1; 168.126.63.2
NTP servers:	Manual	pool.ntp.org; asia.pool.ntp.org; euro
HTTP ports:	Enable	80
HTTPS ports:	Enable	443
RTSP ports:	Enable	554
Enable zero config:	□ 0.0.0.0	
ONVIF discovery mode:	Non-discoverable	

[ONVIF Discovery mode – Apply "Non-discoverable"]

FAQ

Q: How can I find cameras after applying "Non-Discoverable?"

A: To search for a camera after setting the discovery mode to Non-Discoverable, enter the camera's IP address in the ONVIF Device Manager tool to manually connect to a camera. You can then change the ONVIF discovery mode setting back to "Discoverable" as needed.

Hanwha Techwin Co.,Ltd.
Hanwha Techwin R&D Center
13488 Pangyo-ro 319 Beon-gil 6, Sampyeong-dong, Bundang-gu, Seongnam, Gyeonggido
TEL 070.7147.8771-8
FAX 031.8018.3715
http://hanwha-security.com