Hanwha Techwin
Heriot House, Heriot Rd, Chertsey KT16 9DT
hanwha-security.eu

2021 Hanwha Techwin S-Cert Team

9/9/2021

NVR Vulnerability Report

■ OVERVIEW

- ✓ ThroughTek's P2P SDK vulnerabilities have been found as CVE-2021-32934, CVE-2021-28372.
- ✓ Most Hanwha NVRs have been confirmed to use the vulnerable TUTK P2P SDK version. The affected products and firmware is listed in the table below.

- ✓ **CVE-2021-32934**

  ThroughTek supplies multiple original equipment manufacturers of IP cameras & recorders with P2P connections as part of its cloud platform. Successful exploitation of this vulnerability could permit unauthorized access to sensitive information, such as camera audio/video feeds.

- ✓ **CVE-2021-28372**

  ThroughTek's Kalay Platform 2.0 network allows an attacker to impersonate an arbitrary ThroughTek (TUTK) device given a valid 20-byte uniquely assigned identifier (UID). This could result in an attacker hijacking a victim's connection and forcing them into supplying credentials needed to access the victim TUTK device.

■ AFFECTED PRODUCTS AND FIRMWARE

Model	Firmware Version	Release Plan
XRN-2010A XRN-2011A XRN-3010A	2.46 and earlier versions	September
XRN-1610A XRN-1610SA	2.48 and earlier versions	September
QRN-1620S	3.06.12 and earlier versions	November
LRN-410S LRN-810S	3.06.12 and earlier versions	November
XRN-810S XRN-410S QRN-810	2.46 and earlier versions	October

Heriot House, Heriot Rd, Chertsey KT16 9DT
hanwha-security.eu

QRN-410		
XRN-420S QRN-430S	4.10.00 and earlier versions	November
QRN-1610S QRN-810S QRN-410S	2.46 and earlier versions	October
QRN-420S QRN-820S	3.07.11 and earlier versions	November
LRN-1610S	3.06.12 and earlier versions	November
HRX-1621 HRX-1620 HRX-821 HRX-820	3.05.12 and earlier versions	October
HRX-421 HRX-420	3.05.12 and earlier versions	October
HRX-1632 HRX-835 HRX-435 HRX-434	4.09.00 and earlier versions	October
PRN-3210B2 PRN-1610B2 PRN-3200B2 PRN-1600B2 PRN-3205B2 PRN-1605B2	4.04.22 and earlier versions	November
PRN-6410DB4 PRN-6410B4 PRN-3210B4 PRN-6400DB4 PRN-6400B4 PRN-3200B4 PRN-6405DB4 PRN-6405B4 PRN-3205B4	4.05.22 and earlier versions	November
XRN-6410DB4 XRN-6410B4	4.06.22 and earlier versions	November

XRN-3210B4		
XRN-6410RB2 XRN-6410B2 XRN-3210RB2 XRN-3210B2	4.04.22 and earlier versions	November
XRN-1620B2 XRN-1620SB1 XRN-820S	4.07.12 and earlier versions	November
Wisenet Mobile Viewer application	2.2.0 and earlier versions	October

■ RISK ANALYSIS

- ✓ These vulnerabilities are only relevant when adding a device by scanning a QR code or adding a device by manually entering the UID in the Wisenet Mobile viewer application. To resolve this issue, you will need to update to the latest version of both the recorder firmware and the Wisenet Mobile viewer application.
- ✓ If the P2P function is not being used with the Wisenet Mobile Viewer application, such as connections via IP address or DDNS or using other clients, then there is no security risk regarding CVE-2021-32934, CVE-2021-28372.
- ✓ The P2P function can be disabled in the Network menu of the affected recorder. This is advisable until the updated firmware and mobile viewer can be installed.
- ✓ Hanwha recommends that customers update their devices with the latest version firmware. The Wisenet Device Manager can be used to easily download and upgrade firmware to many devices in bulk.
- ✓ The Wisenet Mobile Viewer application can be updated using your device's app store. Automatic updates are recommended to ensure the latest software is available. The Android application can also be downloaded directly from the Hanwha Techwin website.

■ CURRENT STATUS & RELEASE PLAN

- ✓ Since the vulnerability was announced, Hanwha has been working on improvements by getting advice from TUTK on whether the vulnerability exists in our products and how to resolve it.
- ✓ Hanwha will release the fixed firmware according to the schedule in the table above.
- ✓ Hanwha will release the fixed Wisenet Mobile viewer application v2.2.2 in October.

Heriot House, Heriot Rd, Chertsey KT16 9DT
hanwha-security.eu

If you have further questions, or need assistance in updated your device, please contact Hanwha Techwin Technical Support or visit https://www.hanwhas-security.eu/cyber-security/cyber-security/ for additional methods of contacting support.