NCSC under MoD
Research and Development division
support@ims.nksc.lt

REPORT ON THE ASSESSMENT OF CYBER SECURITY OF VIDEO SURVEILLANCE CAMERAS INTENDED FOR HOUSEHOLD USE

The National Cyber Security Centre under the Ministry of National Defence (hereinafter – the NCSC) performed a cyber security assessment of home video surveillance cameras supplied by various manufacturers to the Lithuanian market. The products of Hikvision, Dahua, Xiaomi, TP-Link and Axis Communications intended for the household market with a price range from EUR 33 to EUR 289 were examined during the study (the technical characteristics of the examined cameras are detailed in Annex 1 to the Report). This Report develops and expands on the Report [1] published by the NCSC in May 2020, which identified significant cyber security vulnerabilities in cameras of Chinese manufacturers intended for use in perimeter security systems.

KEY FINDINGS OF THE EXAMINATION

Compared to the cameras examined in the previous study, the newly examined Hikvision and Dahua cameras appeared to have very similar or practically identical technological solutions. The study found that the vulnerability issues of the software of the newly examined cameras, compared to the previously examined products, remain unchanged and pose a threat to the security of the devices. Eleven software packages containing 95 security vulnerabilities were found installed in the Hikvision DS-2CD2183G0-IU camera. Thirty two vulnerabilities had a threat score greater than 6.5 (out of 10). It is worth mentioning that 53 vulnerabilities have been identified in the standard (pre-installed) software of the Swedish Axis Communications camera. The identified vulnerabilities could allow hackers to execute cyber-attacks, remotely intercept camera information and execute malicious code. In addition, the camera was found to be susceptible to Denial of Service (DoS) attacks.

Unlike the tested Chinese cameras, Axis Communications cameras have a software update feature that allows users to install the newest firmware (v 9.3.0) without any known vulnerabilities. The automatic software update functionality did not work correctly in the analysed Hikvision camera. It is important to note that the updates of the Dahua IPC-HFW 1230S-0280B-S1 camera firmware could not be found on the manufacturer's website.

The following systemic security vulnerability was observed in the cameras of Axis Communications, Hikvision and Dahua: the equipment uses HTTP Digest Access Authentication technology that was developed in 1999. This authentication mechanism allows hackers to intercept camera control session information remotely, decrypt and use the user password value for unauthorised camera access.

The management of Xiaomi and TP-Link cameras is based on cloud services using a special mobile application provided by the manufacturer. Using the said application, the user receives camera generated data (video stream, audio track) indirectly via remote third-party servers. The control session is also organised using third-party servers. This poses additional cyber security risks because the user has no control of the servers, infrastructure security and data protection policies used in

camera stream transmission. Open access sources report that under certain conditions, users could see visual information from cameras that did not belong to them. [10]

A comparison of Chinese-designed devices with the Swedish camera revealed that Chinese developers try to implement as much functionality as possible by themselves, applying little-known, exclusive solutions. Chinese manufacturers restrict user access to the camera, prohibit the availability of SSH and/or Telnet services and minimise device accessibility features. This trend has been reported in sources since 2017, when information about security vulnerabilities in Hikvision and Dahua products became the subject of discussion in the press [14] – [17].

The NCSC notes that there is a wide range of products on the market with various security features, and in all cases it recommends real-time auditing of camera port activity and formed requests, blocking redundant requests or flows. That can be done using firewalls with white-lists for a specific camera model. Special measures must be used to ensure the encryption of the streams generated by the camera (media content and service channel) to the information-receiving device (e.g., mobile devices, video security and monitoring systems). The security control of the cameras can be performed with a separate specialised hardware security node connected to the camera via an Ethernet interface, which does not affect or breach the basic functionality of the camera. The function of the security node is to provide real-time camera access control, camera access monitoring, stream anomaly detection, traffic encryption and ensure higher-level cyber security of devices.

TECHNOLOGIAL TEST RESULTS

1. The same security issues are found in Hikvision and Dahua products as in previously tested equipment

A comparative analysis of the products was performed during the study. In the case of Hikvision, the camera Hikvision DS-2CD4C26FWD-AP (that was analysed in May 2020) was compared to a randomly selected newer-edition camera, the Hikvision DS-2CD2183G0-IU. The study revealed that the examined cameras had a common problem, i.e. the software used in the equipment was old and potentially had vulnerabilities. A comparison of the general characteristics of the Hikvision DS-2CD4C26FWD-AP and Hikvision DS-2CD2183G0-IU cameras is shown in Table 1.

Table 1. Comparison of general characteristics of the Hikvision DS-2CD4C26FWD-AP and Hikvision DS-2CD2183G0-IU cameras

No.	Analysed devices		
1	Manufacturer	Hikvision	
2	Test date	May 2020	August 2020
3	Product model	DS-2CD4C26FWD-AP	DS-2CD2183G0-IU
4	Product version	V5.5.84 build 190507	V5.6.2 build 190701
5	Product year	2018	2018
6	Product price, EUR	621	180
7	Number of CVE vulnerabilities	***63***	***95***
8	Number of self-sufficient requests	0	0
9	Number of open ports	5	7
10	Supportability	Supported	Supported

11	ISAPI functionality	Available	Available
12	Authentication algorithm	HTTP-Digest	HTTP-Digest
13	Automatic update feature	Present, but not functioning	Present, but not functioning

A decomposition study of the Hikvision DS-2CD2183G0-IU has shown that the camera runs software solutions that were developed in 2011–2017 with known cyber security vulnerabilities identified in the Commonly Available Vulnerabilities and Exposures (CVE) database. Eleven software packages installed in the camera had 95 vulnerabilities listed in the CVE. Thirty two of those vulnerabilities had a threat score greater than 6.5 (out of 10). That is 34 percent more than in the Hikvision camera examined previously.

Remote interception of camera information and malicious code execution are possible due to the identified vulnerabilities. It was found that the camera is vulnerable to Denial of Service (DoS) attacks. It should also be noted that the newly examined cameras have an automatic software update feature, but attempts to activate the updates were unsuccessful.

In comparison, 63 CVE vulnerabilities were identified in the camera tested in May 2020, twenty-three of which had a threat score greater than 6.5. The software version of the examined camera was 5.5.84, while the newly tested camera had version 5.6.2.

The study revealed that the software databases of the compared cameras are similar to each other, and the fact that more vulnerabilities were identified in the newer version of the software than in the older one may indicate the manufacturer's approach to the cyber security issues of the products it develops. Table 2 lists the potentially insecure software packages used in the Hikvision camera that was tested, including their names, versions, CVE identification number, date of publication of the vulnerability, and threat level of the vulnerability. The results of a previous study of the Hikvision DS-2CD4C26FWD-AP camera are presented in the Report of May 2020 [1].

No.	Software package used in the camera	Version of the package used in the camera	CVE identification number of package vulnerability	Date of publication of the vulnerability	Vulnerability threat score (out of 10)
1	BusyBox	1.19.3	CVE-2018-20679	04/09/2019	5.0
			CVE-2016-6301	09/12/2016	7.8
			CVE-2015-9261	26/07/2018	4.3
			CVE-2013-1813	23/11/2013	7.2
			CVE-2011-2716	03/07/2012	6.8
2	IPTables	1.4.18	CVE-2012-2663	15/02/2014	7.5
3	libxls	1.4.0	CVE-2018-20452	25/12/2018	8.8
			CVE-2018-20450	25/12/2018	6.5
			CVE-2017-2919	01/12/2016	7.8
			CVE-2017-2897	01/12/2016	7.8
			CVE-2017-2896	01/12/2016	7.8
			CVE-2017-12111	31/07/2017	7.8
			CVE-2017-12110	31/07/2017	7.8
			CVE-2017-12109	31/07/2017	8.8
			CVE-2017-12108	31/07/2017	8.8
4	Pauls PPP Package	2.4.3	CVE-2015-3310	24/04/2015	-
			CVE-2014-3158	15/11/2014	-
			CVE-2008-1215	08/03/2008	-

			CVE-2002-0854	05/09/2002	-
			CVE-2002-0851	05/09/2002	-
5	libiconv	1.9.2	CVE-2005-2642	23/08/2005	-
6	WPA_Supplicant	2.6	CVE-2019-16275	12/09/2019	3.3
			CVE-2019-11555	26/04/2019	4.3
			CVE-2019-9499	17/04/2019	6.8
			CVE-2019-9498	17/04/2019	6.8
			CVE-2018-14526	08/08/2018	3.3
			CVE-2017-13088	17/10/2017	2.9
			CVE-2017-13087	17/10/2017	2.9
			CVE-2017-13086	17/10/2017	5.4
			CVE-2017-13084	17/10/2017	5.4
			CVE-2017-13082	17/10/2017	5.8
			CVE-2017-13081	17/10/2017	2.9
			CVE-2017-13080	17/10/2017	2.9
			CVE-2017-13079	17/10/2017	2.9
			CVE-2017-13078	17/10/2017	2.9
			CVE-2017-13077	16/10/2017	5.4
			CVE-2019-9497	17/04/2019	6.8
7	libupnp	1.6.21	-	-	-
8	sqlite	3.7.10	CVE-2019-8457	30/05/2019	7.5
			CVE-2018-20506	03/04/2019	6.8
			CVE-2018-20346	21/12/2018	6.8
9	libssh2	1.8.0	CVE-2019-13115	16/07/2019	5.8
			CVE-2019-3863	25/03/2019	6.8
			CVE-2019-3862	21/03/2019	6.4
			CVE-2019-3861	25/03/2019	6.4
			CVE-2019-3860	25/03/2019	6.4
			CVE-2019-3859	21/03/2019	6.4
			CVE-2019-3858	21/03/2019	6.4
			CVE-2019-3857	25/03/2019	6.8
			CVE-2019-3856	25/03/2019	6.8
			CVE-2019-3855	21/03/2019	9.3
10	protobuf	3.5.1	-	-	-
11	Openssl 1.0.1j	1.0.1j	CVE-2017-3735	28/08/2017	5.0
			CVE-2016-6306	26/09/2016	4.3
			CVE-2016-6304	26/09/2016	7.8
			CVE-2016-6303	16/09/2016	7.5
			CVE-2016-6302	16/09/2016	5.0
			CVE-2016-2842	03/03/2016	10.0
			CVE-2016-2183	31/08/2016	5.0
			CVE-2016-2182	16/09/2016	7.5
			CVE-2016-2181	16/09/2016	5.0
			CVE-2016-2180	31/07/2016	5.0
			CVE-2016-2179	16/09/2016	5.0
			CVE-2016-2178	19/06/2016	2.1
			CVE-2016-2177	19/06/2016	7.5
			CVE-2016-0800	01/03/2016	4.3
			CVE-2016-0799	03/03/2016	10.0
			CVE-2016-0798	03/03/2016	7.8

			CVE-2016-0797	03/03/2016	5.0
			CVE-2016-0705	03/03/2016	10.0
			CVE-2016-0704	02/03/2016	4.3
			CVE-2016-0703	02/03/2016	4.3
			CVE-2016-0702	03/03/2016	1.9
			CVE-2015-4000	20/05/2015	4.3
			CVE-2015-3197	14/02/2016	4.3
			CVE-2015-3196	06/12/2015	4.3
			CVE-2015-3195	06/12/2015	5.0
			CVE-2015-3194	06/12/2015	5.0
			CVE-2015-1792	12/06/2015	5.0
			CVE-2015-1791	12/06/2015	6.8
			CVE-2015-1790	12/06/2015	5.0
			CVE-2015-1789	12/06/2015	4.3
			CVE-2015-1788	12/06/2015	4.3
			CVE-2015-0293	19/03/2015	5.0
			CVE-2015-0289	19/03/2015	5.0
			CVE-2015-0288	19/03/2015	5.0
			CVE-2015-0287	19/03/2015	5.0
			CVE-2015-0286	19/03/2015	5.0
			CVE-2015-0209	19/03/2015	6.8
			CVE-2015-0206	08/012015	5.0
			CVE-2015-0205	08/01/2015	5.0
			CVE-2015-0204	08/01/2015	4.3
			CVE-2014-8275	08/01/2015	5.0
			CVE-2014-3572	08/01/2015	5.0
			CVE-2014-3571	08/01/2015	5.0
			CVE-2014-3570	08/01/2015	5.0
			CVE-2014-3569	24/12/2014	5.0

The enabled and functioning remote control environment ISAPI was found to be operating by default on the examined Hikvision camera. ISAPI *(Intelligent Security Application Programming Interface)* is a protocol used by Hikvision allowing remote control of the device via text requests. This security problem was also identified in the previously examined camera, a more detailed description of which is presented in the NCSC Report of May 2020 [1].

As in the previously examined Hikvision DS-2CD4C26FWD-AP camera, the user access authentication of Hikvision DS-2CD2183G0-IU is performed over an unencrypted connection using a limited-reliability HTTP Digest Access Authentication technology developed in 1999. When the user connects to the camera using this authentication mechanism, the value of the user password can be intercepted. In addition, the user password can be decrypted and used for unauthorised access. It is worth noting that the device has security solutions that allow eliminating the problem of unauthorised user login; however, they were not active in the standard configuration. These vulnerabilities are discussed in detail in the NCSC Report of May 2020 [1]. This authentication mechanism is supported by the ONVIF (*Open Network Video Interface Forum*) standard developed in 2008 [12].

The Hikvision camera ports used for control of camera functions and video feeds are enabled by default. A list of open ports with a description of the functions is presented in Table 3. Compared to the previously examined camera, this camera has two additional Websocket-type ports for communication with the Internet interface. Additional ports are marked in yellow.

Table 3. Open ports in the Hikvision camera. Newly identified ports are marked in yellow

No.	Port	Service	Functionality
1	80/TCP	HTTP	The port is used to access the Web interface. The connection is not encrypted. Possible ISAPI communication.
2	443/TCP	HTTPS	Used to access an encrypted version of the HTTPS Web interface. By default, the header "https://" must be entered in the address field to encrypt the connection to the camera; otherwise an insecure HTTP connection will be used. Possible ISAPI communication.
3	554/TCP	RTSP	The port is used to establish a video feed connection. The software version of the provided service was identified as "Hikvision 7513 POE IP camera rtspd".
4	8000/TCP	Server port	During the connection, a TCP handshake occurs, but after it the port terminates the connection. Adding this port in the Hik-Connect application, present on the local network segment, allows communication with the camera; therefore, it is assumed that the purpose of the port is related to the provision of Hikvision Cloud services.
5	8443/TCP	TCPWRAPPED	During the connection, a TCP handshake occurs, but after it the port terminates the connection. The identified service is "tcpwrapped".
6	7681/TCP	Websocket	The port is used for communication with the Internet interface.
7	7682/TCP	Websocket	The port is used for communication with the Internet interface.

Network monitoring tests did not reveal any standalone requests of the Hikvision camera to remote servers. After the user initiated the plugin download in the administration panel (works with older browsers – IE10, etc.), the camera contacted the German IP address 49.51.129.XXX registered in Germany and downloaded it. The plugin address was identified: http://hikdownload.hik-connect.com/web/webplugin/windows/local-service-components/v1.0.0.0/standard/LocalServiceComponents.exe?timeStamp=1597683420253. The graph of the network traffic generated by the camera during the download is shown in Figure 1.

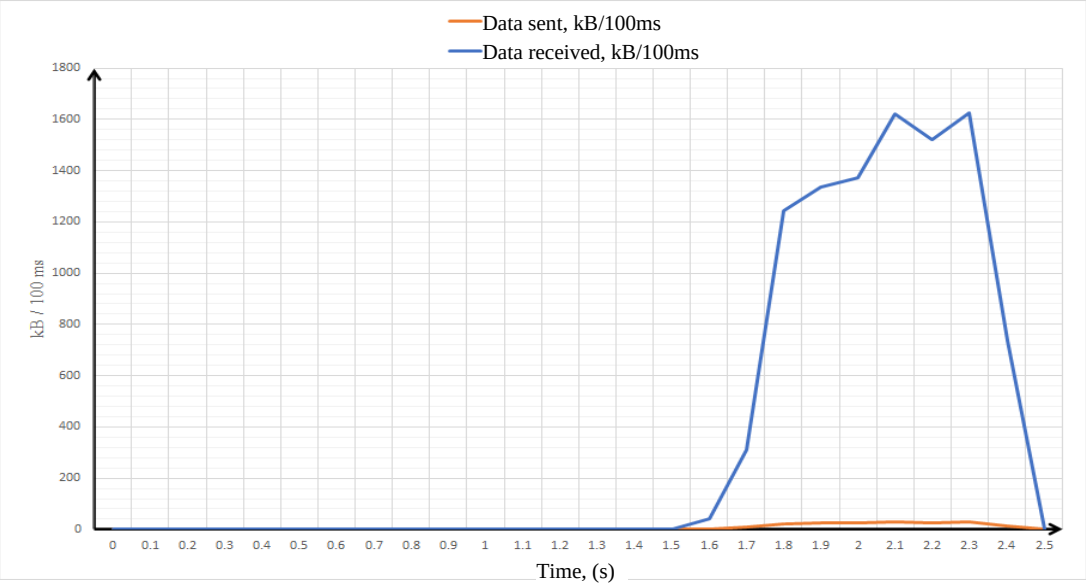


Fig. 1 Hikvision camera network traffic after plugin download initiation

A list of browsers tested with the Hikvision camera during the examination, indicating the year of their development and functional possibilities, is presented in Table 4.

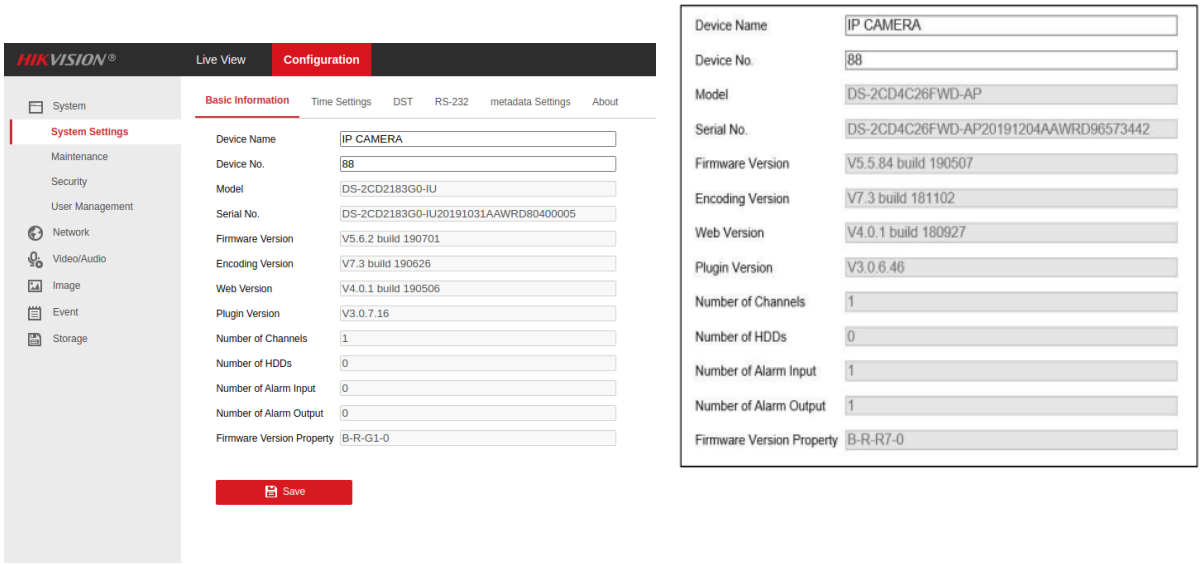
Table 4. List of browsers tested with the Hikvision camera during the examination, indicating the year of their development and functional possibilities

No.	Browser, version, operating system	Browser agent	Date of issue	Success in using control panel of the camera Hikvision DS-2CD4C26FWD-AP *(Study of 05-2020)*	Success in using control panel of the camera Hikvision DS-2CD2183G0-IU *(new study)*
1	Firefox 75 Linux	Mozilla/5.0 (X11; Linux x86_64; rv:75.0) Gecko/20100101 Firefox/75.0	2020	No	Yes
2	Firefox 75 Windows	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:75.0) Gecko/20100101 Firefox/75.0	2020	No	Yes
3	Chrome 81 Linux	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/81.0.4044.122 Safari/537.36	2020	No	Yes
4	Opera 69	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/82.0.4062.3 Safari/537.36 OPR/69.0.3623.0 (Edition developer)	2020	No	Yes
5	Safari 12 Mac OS X	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_4 Supplemental Update) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15	2019	Yes	Yes
6	Edge 44	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36	2019	No	Yes

		Edge/18.17763			
7	Firefox 56	Mozilla/5.0 (Windows NT 6.1; WOW64; rv:56.0) Gecko/20100101 Firefox/56.0	2017	No	Yes
8	Opera 12.14	Opera/12.80 (Windows NT 5.1; U; en) Presto/2.10.289 Version/12.02	2016	Yes	No
9	Firefox 33	Mozilla/5.0 (Windows NT 6.1; WOW64; rv:33.0) Gecko/20120101 Firefox/33.0	2014	Yes	Yes
10	Chrome 34	Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/34.0.1847.116 Safari/537.36 Mozilla/5.0 (iPad; U; CPU OS 3_2 like Mac OS X; en-us) AppleWebKit/531.21.10 (KHTML, like Gecko) Version/4.0.4 Mobile/7B334b Safari/531.21.10	2014	Yes	Yes
11	Internet Explorer 11	Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko	2013	Yes	Yes
12	Safari 7	Mozilla/5.0 (Macintosh; Intel Mac OS X) AppleWebKit/537.75.14 (KHTML, like Gecko) Version/7.0.3 Safari/7046A194A	2013	Yes	No
13	Chrome 19	Mozilla/5.0 (Windows NT 6.0) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.36 Safari/536.5	2012	Yes	No

The examined Hikvision DS-2CD2183G0-IU camera was found to support most of the browsers examined in the study (supported all browsers released since 2017), while the camera examined in the study of May 2020 supported only some of the older browsers. This indicates that the manufacturer is seeking a broader browser compatibility, and work is being done in that direction. A test for compatibility with the manufacturer's mobile application was also conducted. It showed that neither the new HikCentral nor the older Hik-Connect can connect to the camera.

The observed close similarity of the graphical interface of the Hikvision cameras possibly indicates that the manufacturer uses similar or the same technological solutions in different devices. A comparison of the graphical interface of the Hikvision cameras is shown in Figure 2.



Hikvision DS-2CD2183G0-IU Hikvision DS-2CD4C26FWD-AP

Fig. 2. Comparison of Hikvision camera control panels

The following Dahua cameras were examined during the study: Dahua IPC-HFW 1230S-0280B-S1 and Dahua IPC-HDBW2531R-ZS-27135. A comparative analysis with the Dahua DH-IPC-HFW5231EP-ZE camera examined in the NCSC Report of May 2020 [1] was performed.

Table 5. Comparison of general characteristics of the Dahua DH-IPC-HFW5231EP-ZE, Dahua IPC-HFW 1230S-0280B-S1 and Dahua IPC-HDBW2531R-ZS-27135 cameras

No.	**Analysed devices**			
1	Manufacturer	Dahua		
2	Test date	May 2020	August 2020	August 2020
3	Product model	DH-IPC-HFW5231EP-ZE	IPC-HFW 1230S-0280B-S1	IPC-HDBW2531R-ZS-27135
4	System version	V2.800.0000002.0.R, Build Date: 11/01/2019	V2.800.0000005.0.R, Build Date: 25/03/2019	V2.800.0000005.0.R, Build Date: 25/03/2019
5	Web version	V3.2.1.684680	V3.2.1.709882	V3.2.1.709882
6	ONVIF version	16.12(V2.4.3.651299)	16.12(V2.4.3.651299)	16.12(V2.4.3.651299)
7	Security baseline version	1.4	1.4	1.4

Identical Hikvision ISAPI remote control functionality has been found to be enabled by default in all three cameras that are being compared. It is worth noting that the principle of operation of the ISAPI system is that the camera's ISAPI wide-spectrum control environment, activated by default, can potentially be exploited and used for interception of the camera's video streams or otherwise violate user privacy..

The survey revealed that default user authentication in all of the examined Dahua cameras is done through unencrypted communication using a limited-reliability HTTP Digest Access Authentication technology developed in 1999. This problem is also relevant to the Hikvision cameras. The problem was discussed above and is described in detail in the NCSC Report of May 2020 [1]. The Dahua camera ports used for control of camera functions and video streams are enabled by default. A list of open ports with a description of functions is presented in Tables 6 and 7.

Table 6. Open ports in the Dahua IPC-HFW 1230S-0280B-S1 camera

No.	Port	Service	Functionality
1	80/TCP	HTTP	The port is used to access the Web interface. The connection is not encrypted.
2	554/TCP	RTSP	The port is used to send commands to the camera for broadcast, such as STOP or PLAY.
3	1935/TCP	RTMP	This port is used to stream video from the camera without using the Web interface. The port is open, although this feature in the Web environment is disabled by the manufacturer.
4	5000/TCP	UPNP	The UPNP service can be used on this port. The UPNP service, if supported by the router, allows the device to automatically open ports to the external Internet and provide access to the device from external networks without user intervention.

Table 7. Open ports in the Dahua IPC-HDBW2531R-ZS-27135 camera

No.	Port	Service	Functionality
1	80/TCP	HTTP	The port is for access through a web interface. The connection is not encrypted.
2	443/TCP	HTTPS	The port is for access via an encrypted (HTTPS) version of the web interface.
3	554/TCP	RTSP	The port is dedicated for the establishment of a video feed connection.

The mobile application gDMSS Plus of the Dahua camera, dedicated to ensure functionality of camera control, establishes connections to China, Germany and the USA. It has been found that, depending on the device model, the application is able to selectively perform connections. During the examination of the Dahua IPC-HFW1230 camera, the gDMSS Plus connected with 6 IP addresses, located in Ireland (3), Germany (1), the Netherlands (1) and the United States (1). During the examination of the Dahua IPC-HDBW2531R camera, the gDMSS Plus connected with 10 addresses in Germany (7) and China (3).

The gDMSS Plus application connection information from the Dahua IPC-HFW1230 camera examination is presented in Table 8.

Table 8. The gDMSS Plus data exchange information during examination of the Dahua IPC-HFW1230 camera

No.	Address	Country	Amount of data received (Bytes)	Amount of data sent (Bytes)
1	18.195.191.XXX	Germany	13505	0
2	31.13.81.XXX	Ireland	307	289
3	34.250.145.XXX	Ireland	373	260
4	52.49.43.XXX	Ireland	451	573
5	104.87.224.XXX	Netherlands	434	326
6	192.48.236.XXX	USA	596	392

Supplement to the information provided in Table 8, with the dependency on time, from the examination of the Dahua IPC-HFW1230 camera, is presented in Figures 3-5.

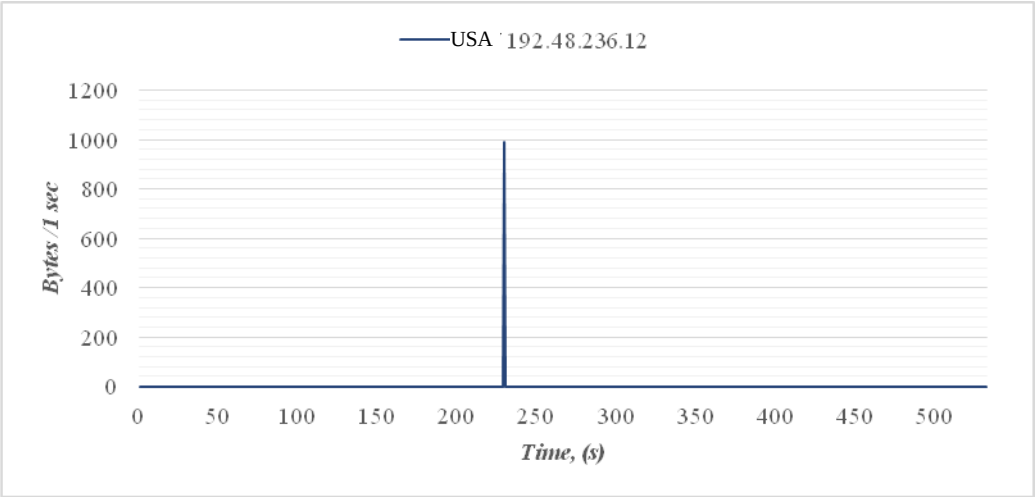


Fig. 3. Two-way TLSv.1.2 communication between the mobile device and the USA server (192.48.236.XXX)

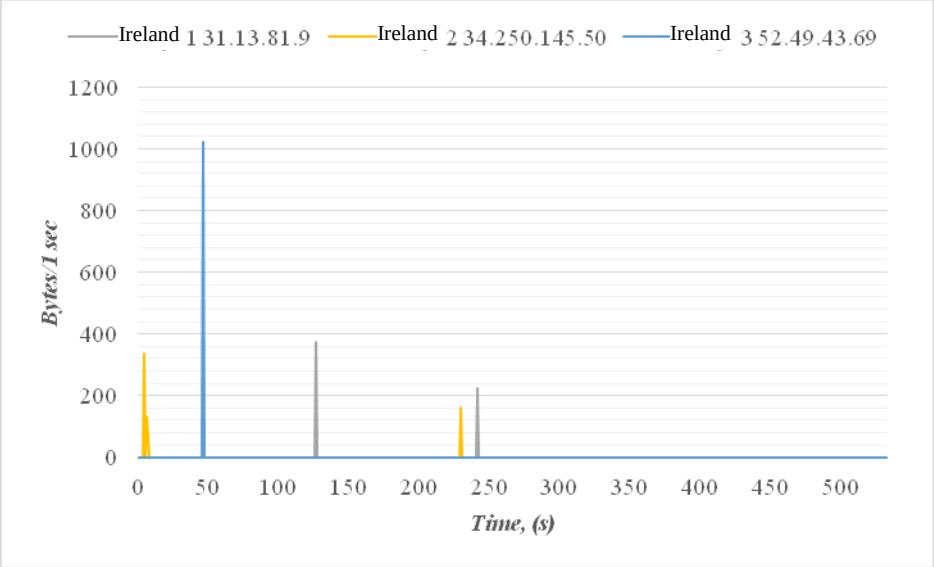


Fig. 4. Two-way TLSv1.2 communication between the mobile device and the servers Ireland 1, Ireland 2 and Ireland 3

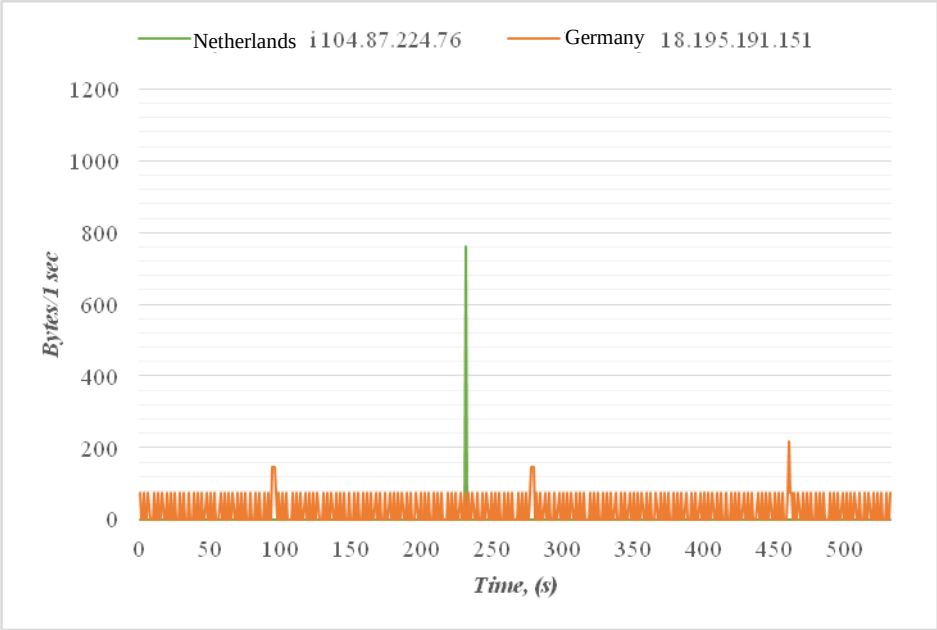


Fig. 5. Two-way communication via TLSv1.2 protocol between the mobile device and the Netherlands server; the UDP protocol requests sent from the mobile device to the Germany server (34.250.145.50).

The gDMSS Plus application connection information from the Dahua IPC-HDBW2531R-ZS-27135 camera examination is presented in Table 9.

Table 9. The gDMSS Plus data exchange information during the examination of the Dahua IPC-HDBW2531R-ZS-27135 camera

No.	Address	Country	Amount of data received (Bytes)	Amount of data sent (Bytes)
1	8.209.65.XXX	Germany	74	0
2	8.209.65.XXX	Germany	74	0
3	8.209.73.XXX	Germany	74	0
4	18.195.191.XXX	Germany	6570	0
5	47.91.91.XXX	Germany	219	723
6	47.91.93.XXX	Germany	74	0
7	47.254.171.XXX	Germany	1194	0
8	114.55.140.XXX	China	691	624
9	116.62.54.XXX	China	2786	1533
10	203.119.128.XXX	China	94	154

Supplement to information provided in Table 9, with the dependency on time, from the examination of the Dahua IPC-HDBW2531R-ZS-27135 camera, is presented in Figures 6-11.

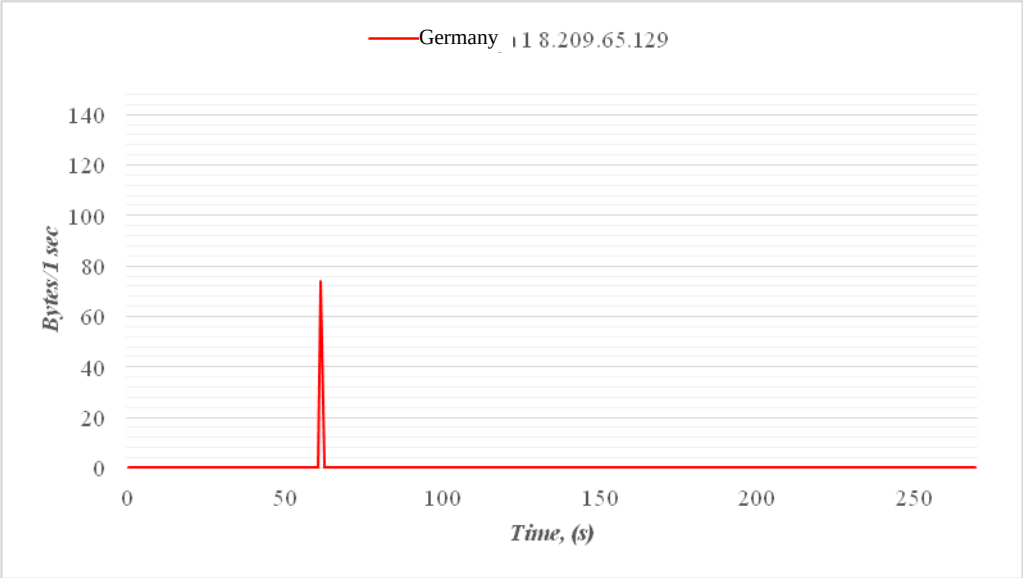


Fig. 6. One TCP package from the mobile device to the server Germany 1 (8.209.65.129)

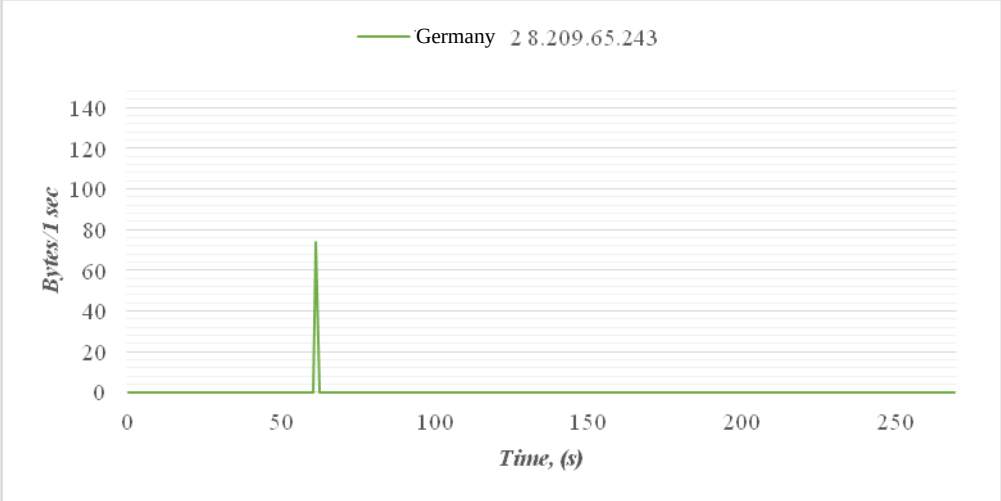


Fig. 7. One TCP package from the mobile device to the server Germany 2 (8.209.65.243)

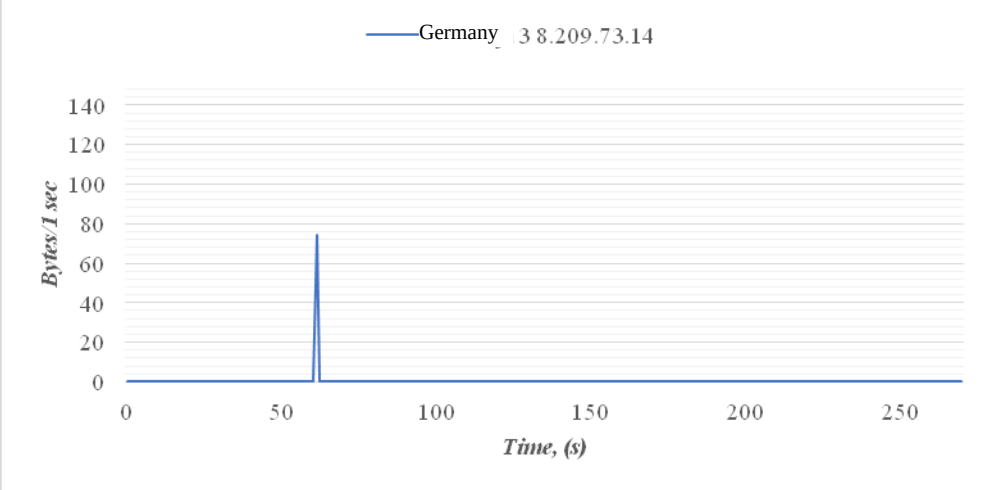


Fig. 8. One TCP package from the mobile device to the server Germany 3 (8.209.73.14)

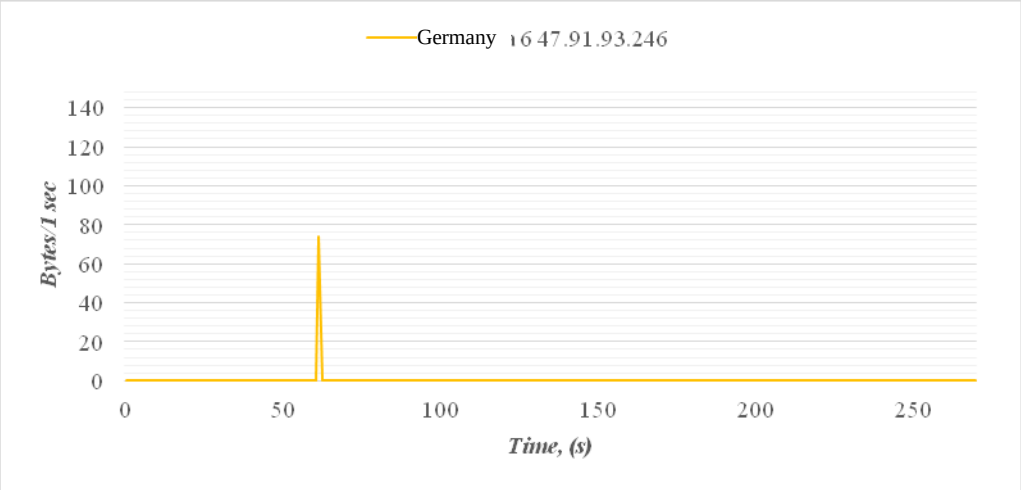


Fig. 9. One TCP package from the mobile device to the server Germany 6 (47.91.93.246)

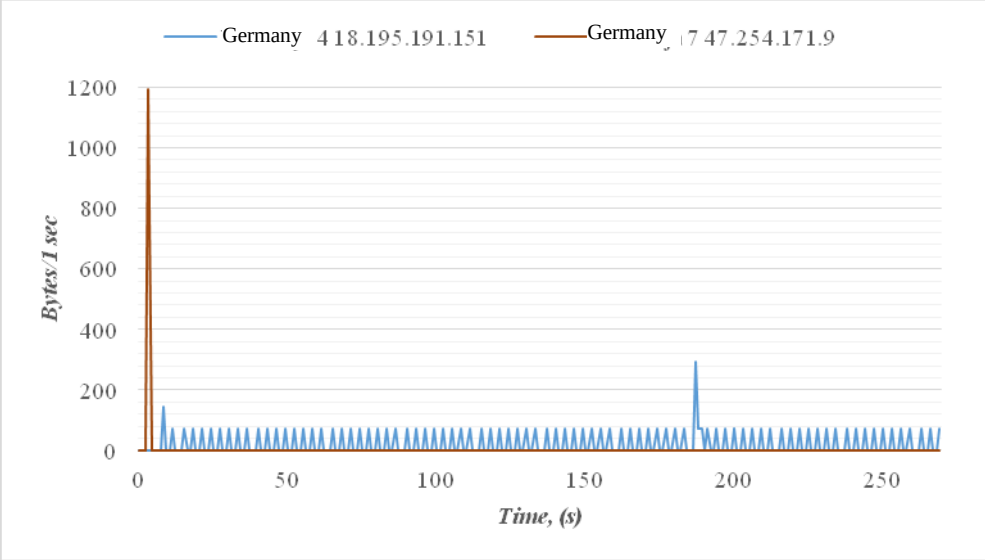


Fig. 10. Continuous sending of device's HTTP requests via UDP protocol to the server Germany 4 (18.195.191.151) and one HTTP request via UDP protocol to the server Germany 7 (47.254.171.9)

The content of the requests to the servers Germany 4 and Germany 7 is presented in Tables 9-10.

Table 9. Content of requests to the server Germany 4

DHGET /online/stun HTTP/1.1

Table 10. Content of requests to the server Germany 7

GET /p2p/stun/probe HTTP/1.1 Content-Type: Content-Length: 89 <body><replaceHost>0</replaceHost><replacePort>0</replacePort><seq>566783010</seq></body>

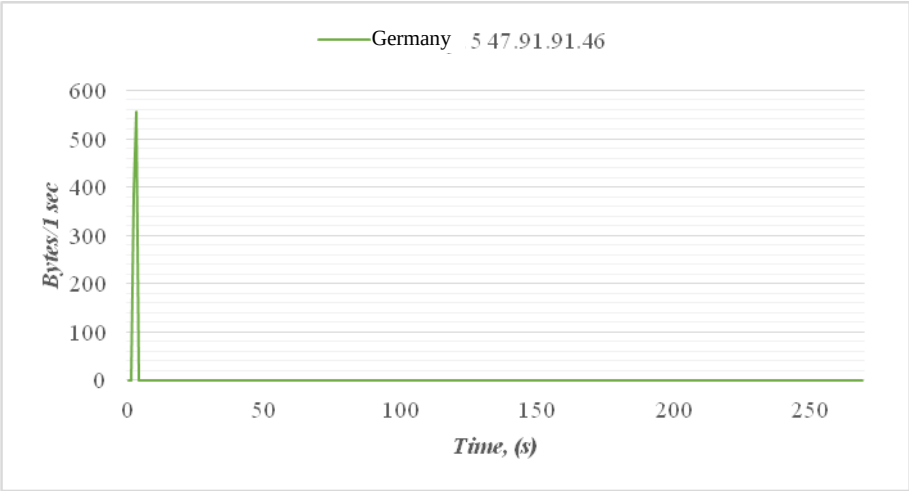


Fig. 11. Two-way UDP communication between the mobile device and the server Germany 5 (47.91.91.46)

Table 11 provides information on requests to the server Germany 5 and responses to the device. The request to the server is marked in red and the response is marked in blue.

Table 11. Request to the server Germany 5 and response received

DHGET /online/stun HTTP/1.1

HTTP/1.1 200 OK
Date: 2020-05-25T20:44:54+08:00
CSeq: 0
Content-Type:
Content-Length: 101

<?xml version="1.0" encoding="UTF-8"?><body><STUN>47.254.171.9:8810</STUN><PortNum>6</PortNum></body>

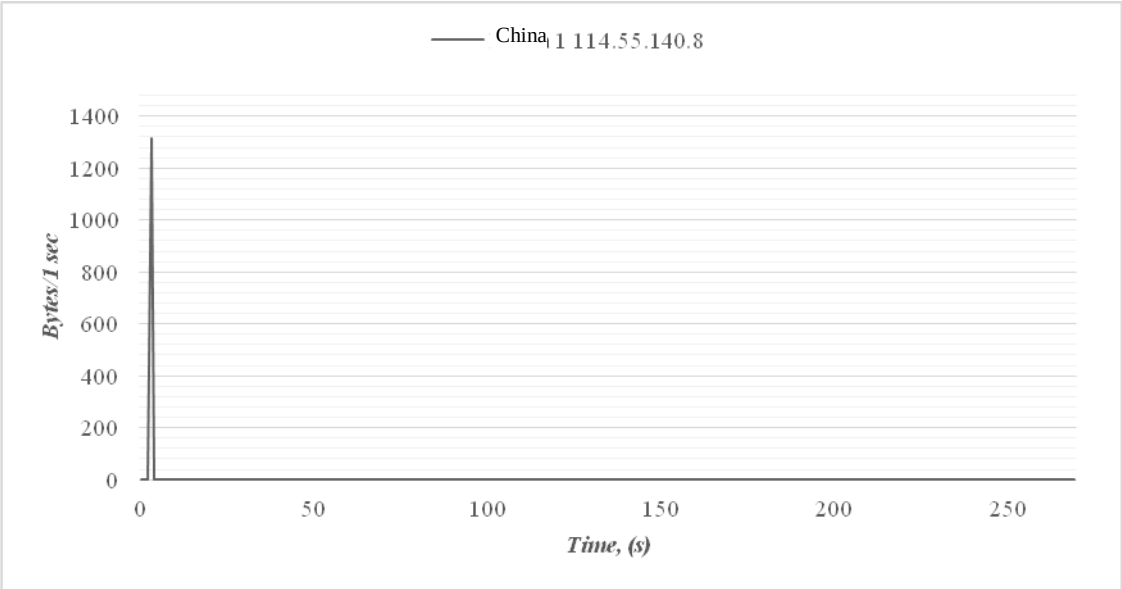


Fig. 12. Two-way UDP communication between the mobile device and the server China 1

Table 12 provides information on requests to the server China 1 and responses to the device. The request to the server is marked in red and the response is marked in blue.

Table 12. Request to the server China 1 and response received

```
DHGET /online/stun HTTP/1.1

HTTP/1.1 200 OK
CSeq: 0
Content-Type:
Content-Length: 101

<?xml version="1.0" encoding="UTF-8"?><body><STUN>116.62.54.73:8810</STUN><PortNum>6</PortNum></body>
```

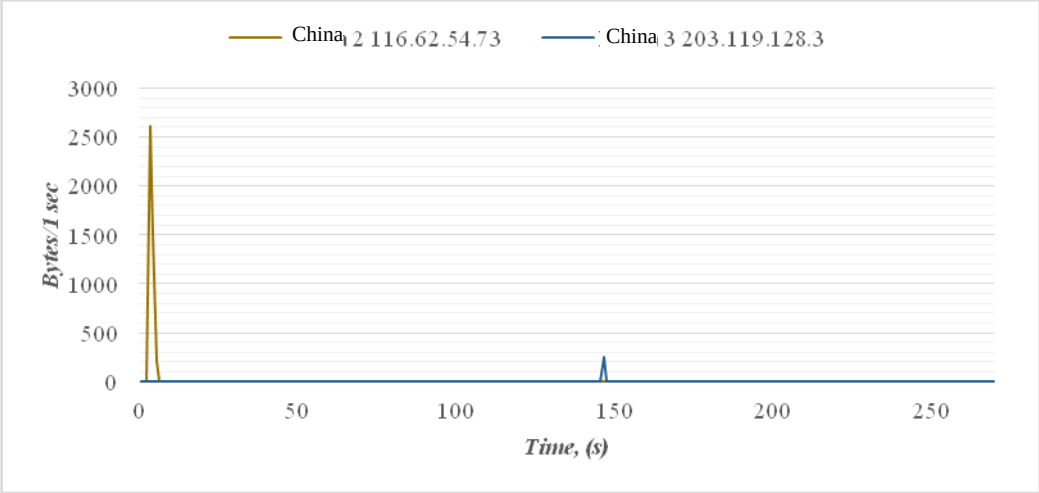


Fig. 13. Two-way UDP communication between the mobile device and the server China 2

Table 13 provides information on requests to the server China 2 and responses to the device. The request to the server is marked in red and the response from the server is marked in blue.

Table 13. Request to the server China 2 and response received

```
GET /p2p/stun/probe HTTP/1.1
Content-Type:
Content-Length: 89

<body><replaceHost>0</replaceHost><replacePort>0</replacePort><seq>951691999</seq></body>GET /p2p/stun/probe HTTP/1.1
Content-Type:
Content-Length: 89

<body><replaceHost>0</replaceHost><replacePort>0</replacePort><seq>951691999</seq></body>HTTP/1.1 200 OK
CSeq: 0
Content-Type:
Content-Length: 112
```

<?xml version="1.0" encoding="UTF-8"?><body><seq>951691999</seq><ip>195.182.88.130</ip><port>23165</port></body>HTTP/1.1 200 OK
CSeq: 0
Content-Type:
Content-Length: 112

<?xml version="1.0" encoding="UTF-8"?><body><seq>951691999</seq><ip>195.182.88.130</ip><port>23165</port></body>

Table 14 provides information on requests to the server China 3 and responses to the device. The request to the server is marked in red and the response from the server is marked in blue.

Table 14. Request to the server China 2 and response received. The contents of the request and response were not readable.

...$...'
$..v/..T.L.....kFt.

...$....<.u...O..0_..
.7e].#.G...-.....

The gDMSS Plus mobile application was examined more thoroughly by the NCSC in the Report of May 2020, in which it was found that the application selectively performs connections depending on the country in which it is located. After summarising the study of the operation of this application, no direct cyber security vulnerabilities were identified; however, it was observed that the mobile application creates connections with servers located in the USA, Germany, Ireland, the Netherlands and China.

Configuration files were detected in the cameras, which potentially describe the compatibility of the software with the hardware. An image extract of the configuration file is shown in Table 15.

Table 15. Image extract of the configuration file

<...>
"IPC-HFW2231R-ZS-2713:01:02:02:4A:25:00:01:00:00:00:00:04:2D0:00:00:00:00:00:00:01:00:00:100",
"IPC-HDW2231RP-ZS-2713:01:02:05:4A:25:00:01:00:00:00:00:04:2D0:00:00:00:00:00:00:01:00:00:100",
"IPC-HFW2231R-ZS-2713:01:02:02:4A:25:00:01:0F:01:01:04:2D0:03:00:00:00:00:01:00:00:100",
"IPC-HDW2230RP-ZS:01:02:05:4F:20:00:01:00:00:00:00:04:2D0:00:00:00:00:00:00:01:00:00:100",
"IPC-HDBW2230R-Z:01:02:05:4F:20:00:01:0E:01:01:04:2D0:03:00:00:00:00:01:00:00:100",
"IPC-HDBW2230R-VF:01:02:05:4F:20:00:01:0E:01:01:04:2D0:03:00:00:00:00:01:00:00:100",
"IPC-HDBW2230R-Z:01:02:05:4F:20:00:01:00:00:00:00:04:2D0:00:00:00:00:00:00:01:00:00:100",
"IPC-HDBW2230R-VF:01:02:05:4F:20:00:01:00:00:00:00:04:2D0:00:00:00:00:00:00:01:00:00:100",
"IPC-HDBW2230R-Z:01:02:05:4F:25:00:01:0E:01:01:04:2D0:03:00:00:00:00:01:00:00:100",
"IPC-HDBW2230R-VF:01:02:05:4F:25:00:01:0E:01:01:04:2D0:03:00:00:00:00:01:00:00:100",
"IPC-HDBW2230R-Z:01:02:05:4F:25:00:01:00:00:00:00:04:2D0:00:00:00:00:00:00:01:00:00:100",
"IPC-HDBW2230R-VF:01:02:05:4F:25:00:01:00:00:00:00:04:2D0:00:00:00:00:00:00:01:00:00:100",
"IPC-HDBW2230R-Z-2713:01:02:05:4F:25:00:01:0E:01:01:04:2D0:03:00:00:00:00:01:00:00:100",
<...>

It can be assumed that the same software is used in different cameras; the software of the tested camera is potentially suitable for the models in the list.

The user interface is realised in Sonia through a statically compiled C ++ program. While

restoring the functionality of the program, entries have been found suggesting that the program is compiled from several libraries that require very old versions of the GNU C Library (glibc 2.4, glibc 2.7, glibcxx 3.4.15, glibcxx 3.4.9, glibcxx 3.4.20, glibcxx 3.4.21). These versions have 15 CVE-marked vulnerabilities.

The functionality of the IPC-HFW 1230S-0280B-S1 and IPC-HDBW2531R-ZS-27135 has been found to be very similar. Observed functional differences –include: the camera IPC-HDBW2531R-ZS-27135 additionally has a recording function, zoom and focus settings, SD card unexpected event detection and notification, alarm option when creating a camera work schedule, and storage of recordings on the SD card.

Software update on the cameras could not be activated; UI returned an error message after t = 5 (s): Check time is out.

2. The Xiaomi and TP-Link cameras operate on the basis of cloud computing; data exchange takes place through third-party servers

The study compared cameras of other Chinese manufacturers, such as the Xiaomi Mi Home 360 1080p and the TP-Link Tapo C200. These cameras are designed for household use and the price of the products is approx. EUR 30. These cameras are characterised by the fact that they are accessible only through cloud computing platforms.

Table 16. Comparison of the general characteristics of Xiaomi Mi Home 360 1080p and TP-Link Tapo C200

No.	Analysed devices		
1	Manufacturer	Xiaomi	TP-Link
2	Product model	Mi Home 360 1080p	Tapo C200
3	Product version	3.4.2_0077	V5.6.2 build 190701
4	Product year	2018	2020
5	Product price, EUR	33	32
6	Number of CVE vulnerabilities	0	1
7	Supportability	Supported	Supported
8	Number of open ports	0	0
9	Availability	Only via official mobile application or cloud computing platform	

It is necessary to use the manufacturer's application Mi Home on the mobile device to control the Xiaomi Mi Home 360 1080p camera. When the camera is connected to the Internet, all its control is performed via the mobile application that handles requests to the Xiaomi cloud computing platform. This platform, after receiving requests from mobile applications, sends control commands to the camera. It was found that the mobile application and the camera make requests to different servers. Table 17 shows the addresses contacted by the camera and the mobile application.

Table 17. Requests of the Xiaomi Mi Home 360 1080p camera and the controlling mobile application Mi Home

No.	Address / domain	Country	Data exchange speed, kB/s	Data link object
1	3.124.122.199	Germany	0.05	Xiaomi camera
2	47.254.176.66	Germany	0.05	
3	8.211.43.167	Singapore	0.07	

4	47.91.76.21	USA	0.075	
5	de.api.io.mi.com	Germany	9	Mobile application
6	de.buisiness.smarcamera.api.io.mi.com	Germany	7	
7	data.mistat.xiaomi.com	Singapore	1	

The mobile application sends control requests to servers in Germany (2) and Singapore (1), which transform them into camera control requests via the cloud platform and forward them through the secondary servers in Germany (2), Singapore and the USA. An associative operation diagram of the system when the controlling mobile application and the camera are connected to the local network is shown in Figure 14.

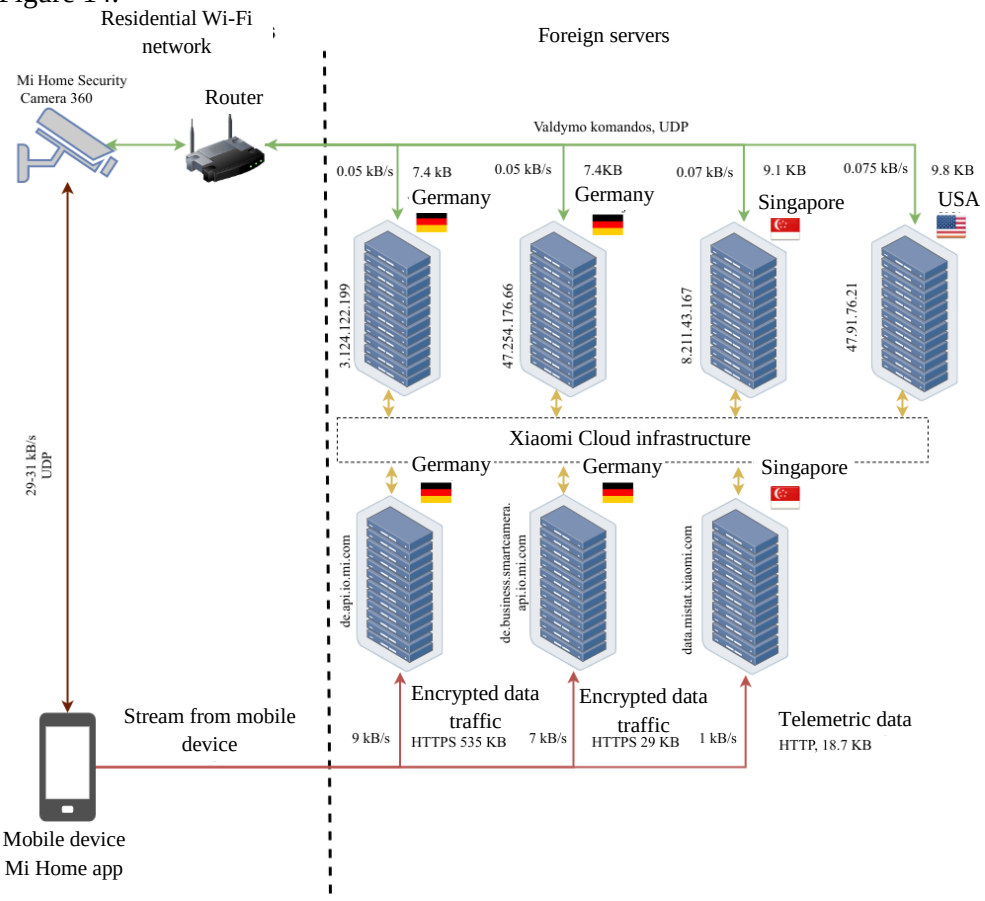


Fig. 14. Associative diagram of Xiaomi camera operation, when the camera and the mobile application that controls it are connected to a local network

The camera performs a continuous data exchange with Xiaomi infrastructure, i.e. periodically makes requests to IP addresses 3.124.122.199 (Germany), 47.254.176.66 (Germany), 8.211.43.167 (Singapore), 47.91.76.21 (USA).

It can be argued that a constantly maintained session (or the creation of new ones) allows for a relatively quick response to commands coming from the Xiaomi cloud infrastructure. Network flow graphs denoting periodic camera requests to the servers are shown in Figures 15-18.

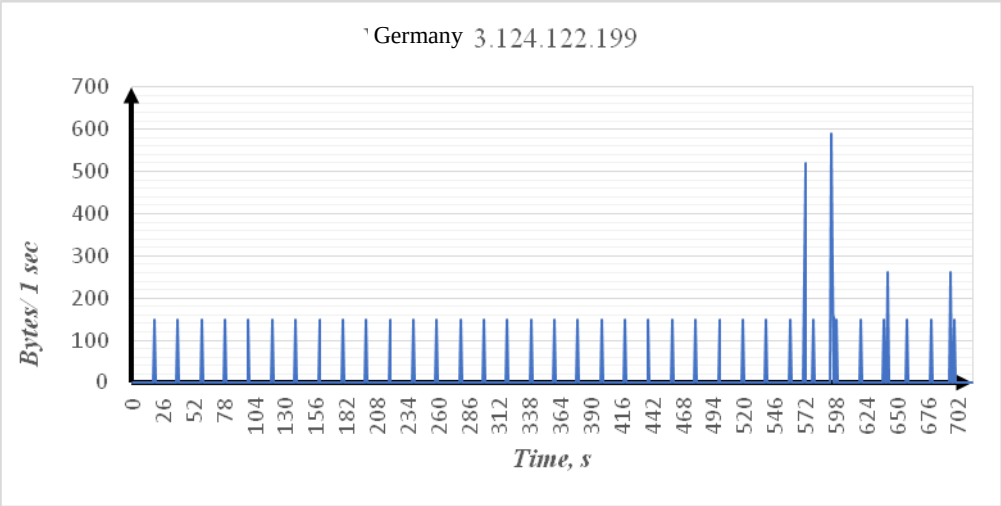


Fig. 15. Xiaomi periodic server requests to the server 3.124.122.199 (Germany)

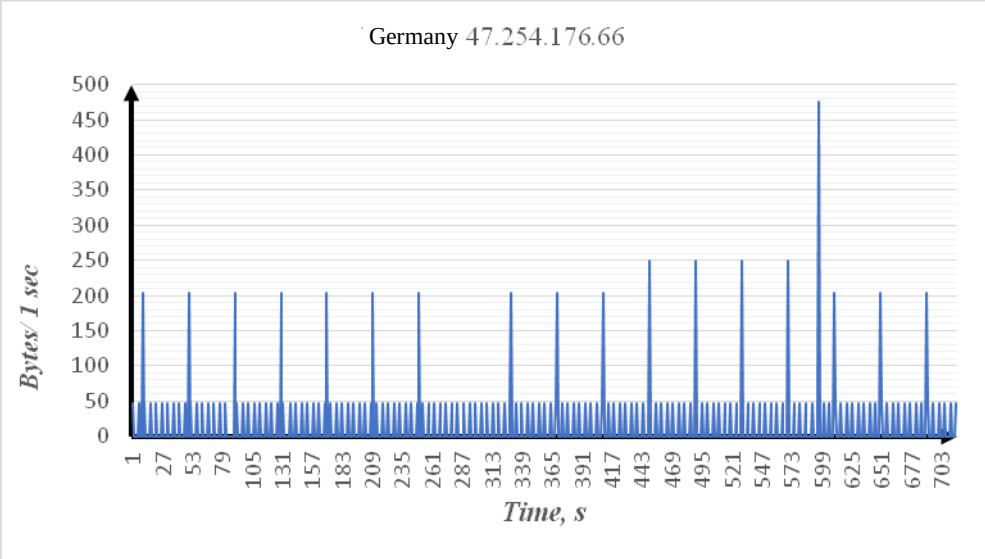


Fig. 16. Xiaomi periodic server requests to the server 47.254.176.66 (Germany)

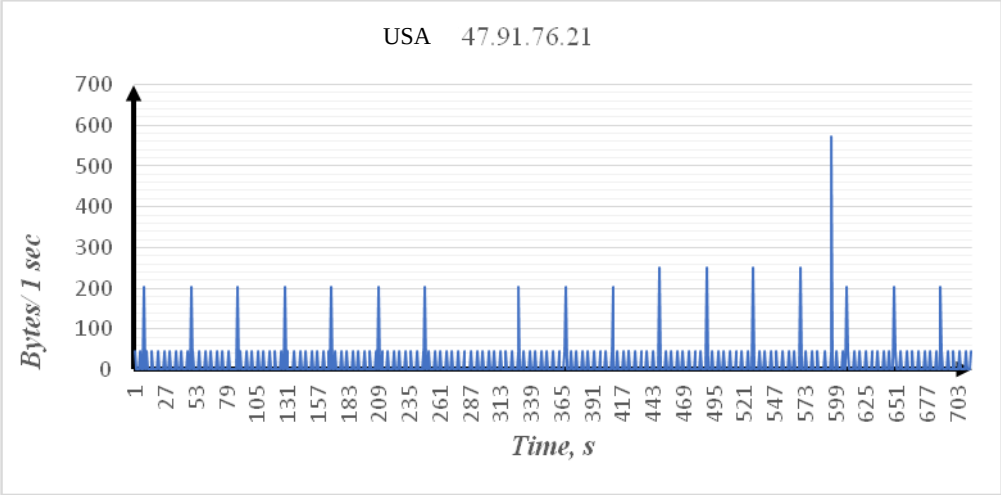


Fig. 17. Xiaomi periodic server requests to the server 47.91.76.21 (USA)

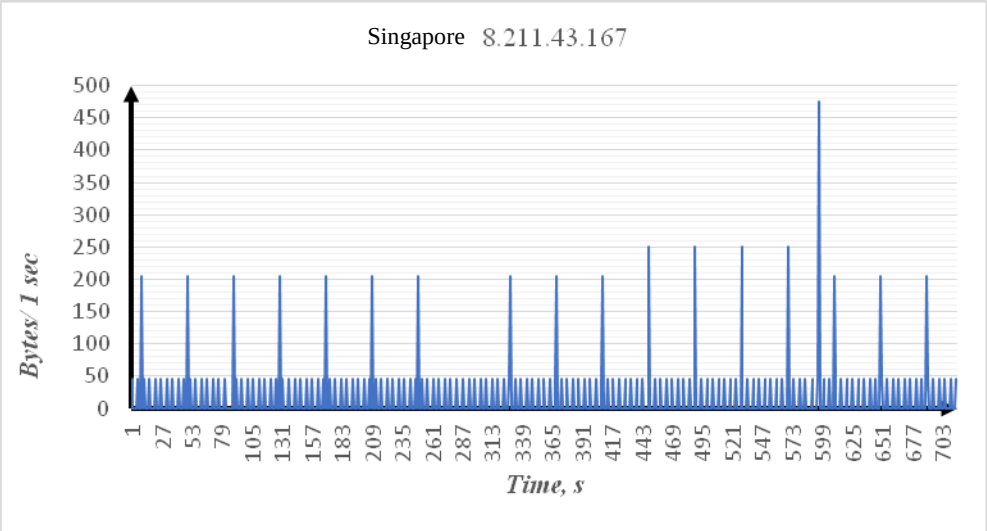


Fig. 18. Xiaomi periodic server requests to the server 8.211.43.167 (Singapore)

The graphs show a well-expressed periodic characteristic of the camera's access to remote servers. Constant communication with remote infrastructure servers can potentially increase security risks; requests to servers are not controlled, they are sent periodically, and camera control commands received from the servers are not verified by the camera administrator (user).

The mobile control application in standby mode sends 32 byte packets identical to the specified addresses via the UDP protocol. It is believed that, as do the cameras, the application maintains a constant connection with Xiaomi servers in this way.

It was found that when the camera and mobile control application are on the local network, the camera is controlled via the Xiaomi cloud infrastructure, and the image is broadcast to the mobile application on the local network, directly (without using third-party infrastructure and without connecting to remote servers).

The camera having no direct connection to the mobile application, all data exchange (including camera-generated audiovisual content) is performed using Xiaomi cloud infrastructure. A diagram of this case is presented in Figure 19.

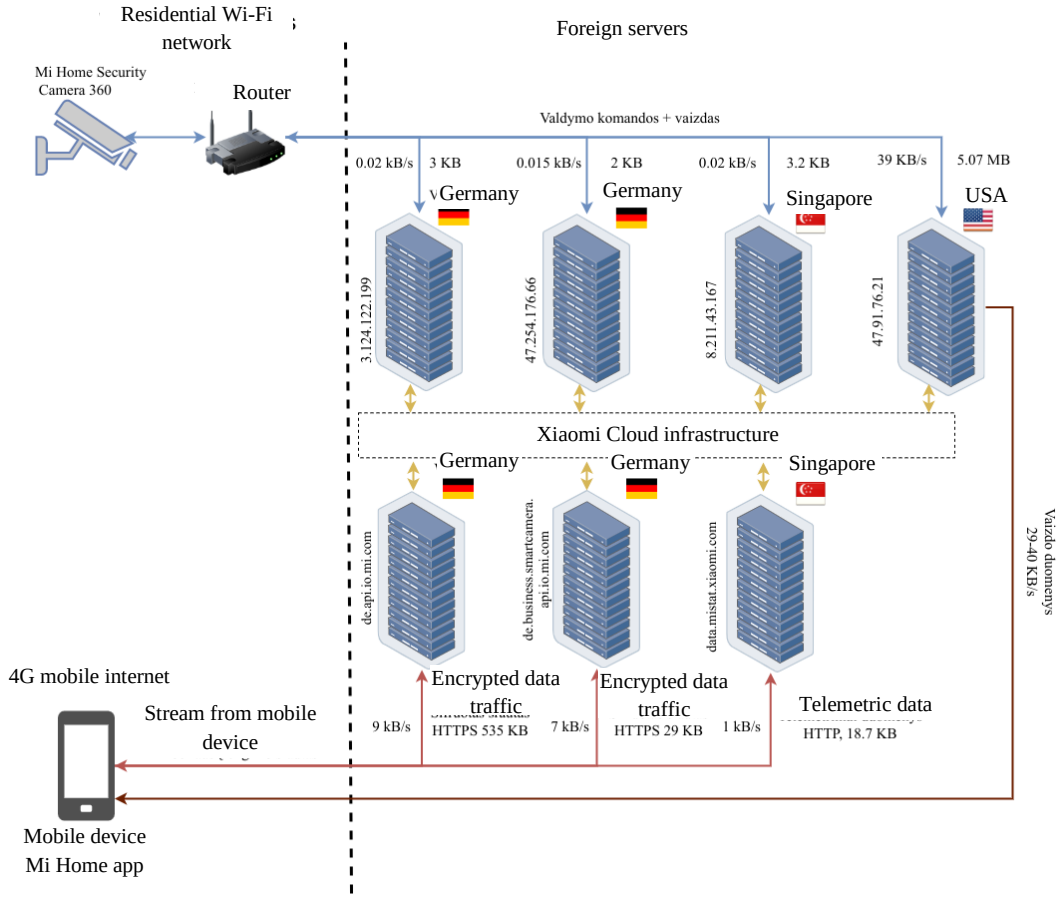


Fig. 19. The camera and the control application are not connected through the local network

In this case, the camera executed requests to the same servers with the same periodic request characteristics. After initiating real-time camera video viewing in the mobile application, the camera began broadcasting content to the server in the USA at IP address 47.91.76.21. After the broadcast began, the application, receiving a control signal from Xiaomi infrastructure, connected to the server in the USA and began the process of receiving content, performing procedures for downloading material from a remote server, and decoding and retrieving of content. Information about data exchange between the camera, Xiaomi infrastructure and the mobile application is provided in Table 18.

Table 18. Information about data exchange between the Xiaomi Mi Home 360 1080p camera, Xiaomi infrastructure and the mobile application

No.	Address / domain	Country	Data exchange speed, kB/s	Data link object
1	3.124.122.199	Germany	0.05	Camera
2	47.254.176.66	Germany	0.05	
3	8.211.43.167	Singapore	0.07	
4	47.91.76.21	USA	39	
5	de.api.io.mi.com	Germany	9	Mobile device
6	de.buisiness.smarcamera.api.io.mi.com	Germany	7	
7	data.mistat.xiaomi.com	Singapore	1	
8	47.91.76.21	USA	39	

The security uncertainty of such a system is also exacerbated by information found in sources that, under certain conditions, users can see visual information from cameras not belonging to them [10]. Other researchers note that a bug was found in the mobile control application, allowing Google Home devices unauthorised access to devices not belonging to the users [13].

The study found that several telemetry data acquisition and transmission modules are integrated into the application. Some of them, such as Onetrack, are included in the application, but do not work. The main active telemetry module is Mistats. It has its own database created to store intermediate results. Based on the request structure of the application, it can be said that the photos and videos captured by the camera are stored in the Xiaomi cloud, and from there they are sent to the control application. An image of the downloading of photos or video captured by the camera is shown in Fig. 20. Figure 21 shows the response from the server.

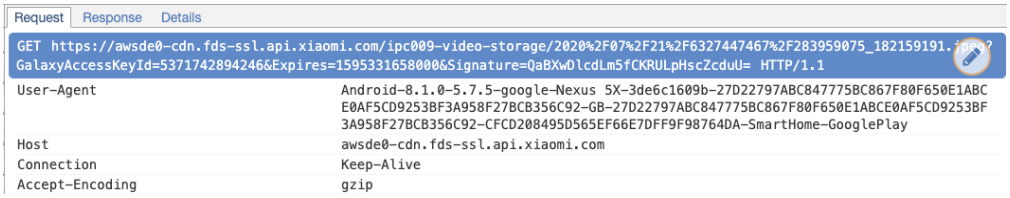


Fig. 20. Request to download recorded images or videos from the camera

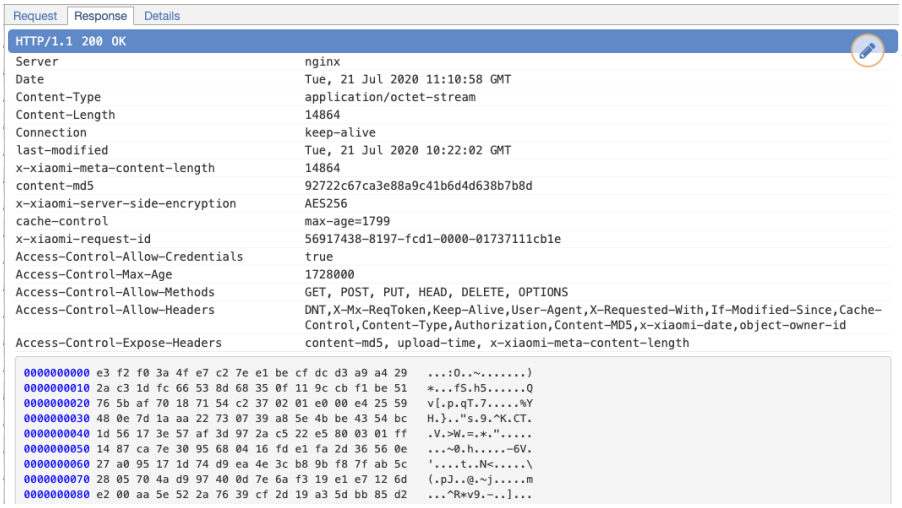


Fig. 21. The response provided by the Xiaomi server

During the examination of the TP-Link Tapo camera in the study, the mobile application contacted 10 addresses: 8 in Ireland and 2 in the USA. Reference information is presented in Table 19.

Table 19. TP-Link Tapo camera remote server request information

No.	Address	Domains	Country	Amount of data received (Bytes)	Amount of data sent (Bytes)
1	18.203.183.110	n-wap-gw.tplinkcloud.com	Ireland	44268	47577
2	34.247.35.149	n-euw1-resources.tplinkcloud.com	Ireland	1802	3483
3	34.251.0.252	app-server.iot.i.tplinknbu.com	Ireland	4165	13282
4	52.18.11.166	app-server.iot.i.tplinknbu.com	Ireland	28219	48043
5	52.31.161.155	app-server.iot.i.tplinknbu.com	Ireland	13614	37045

6	52.208.176.236	n-wap-gw.tplinkcloud.com	Ireland	18714	16855
7	52.216.240.164	prd-tplinknbu-com-store-use1.s3.amazonaws.com	USA	76026	2488563
8	54.72.191.203	analytics.tplinkcloud.com	Ireland	10052	28213
9	54.77.152.116	analytics.tplinkcloud.com	Ireland	4012	11414
10	54.230.228.11	tapo.com	USA	14036	273862

The mobile application TP-Link Tapo demands permissions from the phone's camera, geolocation, microphone, and user files.

It is worth noting that the SSL Pinning attack test failed to bypass the camera's security. Upon successful connection to TLS 1.3, the created channel was terminated immediately. It is believed that TP-Link has implemented additional protections and checks at the application level to ensure communication security.

3. The Axis M3044-V View camera uses open source upgradable solutions

Fifty-three CVE vulnerabilities were identified in the standard Axis Communications camera software (version v1.x). It is important to note that the camera has software update functionality that installs the latest version of the software without known vulnerabilities. Table 20 summarises the characteristics of the Axis Communications camera, comparing software versions from 2017 (version 7.3.0) and 2019 (version 9.3.0).

Table 20. Key features of the Axis Communications camera Axis M3044-V View, noting security differences in software packages

No.	**Analysed device**		
1	Manufacturer	Axis Communications	
2	Product model	Axis M3044 –V View	
3	Software version	7.3.0	9.3.0
4	Version release year	2017	2019
6	Number of CVE vulnerabilities	53	0
7	Supportability	Supported	Supported
8	Number of open ports	1	1

Fifty-three CVE security vulnerabilities have been identified in the software version included in the standard camera package. Information about the identified security vulnerabilities in software version 7.3.0 is presented in Table 21.

Table 21. Security vulnerabilities identified in the Axis Communications camera software version 7.3.0

No.	Software package used in the camera	Version of the package used in the camera	CVE identification number of package vulnerability	Date of publication of the vulnerability	Vulnerability threat score (out of 10)
	Apache2	2.4.25	CVE-2019-10098	25/09/2019	5.8
			CVE-2019-10092	26/09/2019	4.3
			CVE-2019-10082	26/09/2019	6.4

			CVE-2019-10081	15/08/2019	5.0
			CVE-2019-0220	11/06/2019	5.0
			CVE-2019-0211	08/04/2019	7.2
			CVE-2019-0197	11/06/2019	4.9
			CVE-2019-0196	11/06/2019	5.0
			CVE-2018-17199	30/01/2019	5.0
			CVE-2018-11763	25/09/2018	4.3
			CVE-2018-1333	18/06/2018	5.0
			CVE-2018-1312	26/03/2018	6.8
			CVE-2018-1283	26/03/2018	3.5
			CVE-2017-15715	26/03/2018	6.8
			CVE-2017-15710	26/03/2018	5.0
			CVE-2017-9798	18/09/2017	5.0
			CVE-2017-9788	13/07/2017	6.4
			CVE-2017-7679	19/06/2017	7.5
			CVE-2017-7668	19/06/2017	7.5
			CVE-2017-7659	26/07/2017	5.0
			CVE-2017-3169	19/06/2017	7.5
			CVE-2017-3167	19/06/2017	7.5
2	BusyBox	1.24.2	CVE-2018-20679	09/01/2019	5.0
			CVE-2016-6301	09/12/2016	7.8
			CVE-2016-2148	09/02/2017	7.5
			CVE-2016-2147	09/02/2017	5.0
			CVE-2015-9261	26/07/2018	4.3
3	bzip2	1.0.6	CVE-2019-12900	19/06/2019	7.5
			CVE-2016-3189	30/06/2016	4.3
4	cryptsetup	1.7.2	CVE-2016-4484	23/01/2017	7.2
5	dosfstools	2.11	CVE-2016-4804	03/06/2016	2.1
			CVE-2015-8872	03/06/2016	2.1
6	e2fsprogs	1.43	CVE-2019-5094	24/09/2019	4.6
			CVE-2015-1572	24/02/2015	4.6
			CVE-2015-0247	17/02/2015	4.6
7	gstreamer	1.10.4	CVE-2020-6095	27/03/2020	7.5
			CVE-2019-9928	24/04/2019	8.8
			CVE-2017-5848	09/02/2017	7.5
			CVE-2017-5847	09/02/2017	7.5
8	iproute2	4.9.0	CVE-2019-20795	09/05/2020	6.7
9	iptables	1.6.0	CVE-2019-9946	02/04/2019	7.5
			CVE-2019-9735	12/03/2019	6.5
			CVE-2019-11360	12/07/2019	5.5
			CVE-2018-19986	13/05/2019	9.8
			CVE-2017-8217	25/04/2017	5.3
			CVE-2017-7543	26/07/2018	5.9
			CVE-2017-6079	16/05/2017	9.8
			CVE-2017-18017	03/01/2018	9.8
			CVE-2016-9599	23/04/2018	7.5
10	backbone	1.3.3	CVE-2016-5475	21/07/2016	7.6
			CVE-2016-5474	21/07/2016	8.8

			CVE-2016-10537	31/05/2018	5.4
			CVE-2014-2073	10/04/2018	9.8

The camera uses a large number of open source solutions. According to documentation published by Axis Communications0, it can be stated that the Swedish company informs customers about software vulnerabilities detected in the equipment and publicly presents information about measures on how to fix them. This is supported by the fact that the camera manufacturer has released software update 9.3.0 with no known security vulnerabilities. The software packages used in the software update are iptables v1.8.3, busybox v1.31.0, Apache v2.4.43, OpenSSL v1.1.1g, CryptSetup v2.2.1, GStreamer v1.16.1, Backbone.js v1.4.0. Software packages that had vulnerabilities in the older version of the system have been removed (bzip2 package) or have been replaced with equivalents. Security updates for this camera are scheduled till 2025, although production of the model has ceased.

In the Axis Communications camera that was examined, user authentication is done by default through unencrypted communication using a limited-reliability HTTP Digest access authentication technology created in 1999. This problem is also relevant in the Hikvision and the Dahua cameras, it was discussed above and described in detail in the NCSC Report of May 2020 [1].

It is worth noting that Axis supports encryption functionality for the SD card inserted in the camera. A graphical representation of the card encryption interface is shown in Figure 22.

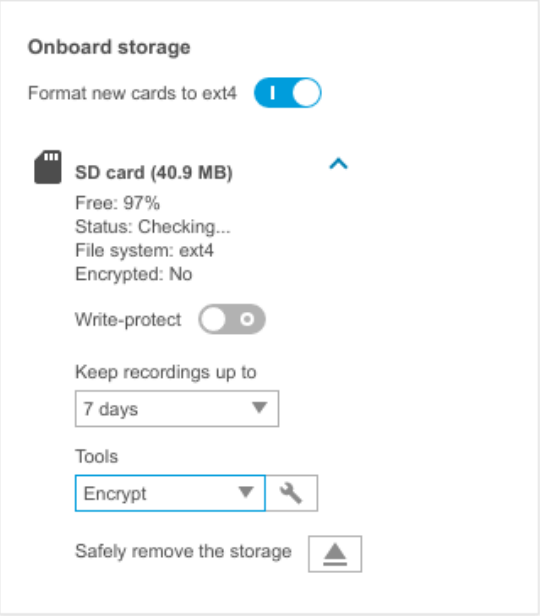


Fig. 22. Graphical image of the SD card encryption interface

The AES-128 used for encryption ensures a high level of data security and is enabled by the resources of the processor used.

The study found that 4 out of the 6 cameras tested use chips from US manufacturer Ambarella. 3 of the tested cameras use the S3L-N-B0-RH chip. Different manufacturers make cameras with different RAM and FLASH configurations. Typically, the main image processing chip is supplemented with DDR3 RAM. Parallel FLASH memory is also often used. All cameras are implemented with a pulse-type power supply circuit. Cameras that support a microSD card usually

need to be disassembled (the top of the case is removed) in order to install a microSD card.

RECOMMENDATIONS

It is recommended to isolate video surveillance cameras in a separate physical or specifically parametrised logical network that does not have access to service, local, or public Internet networks.

It is recommended that organisations do not reveal their identities or download updates from remote non-NATO or non-EU servers. A good solution would be to organise the distribution of software updates from servers registered in Lithuania, which would contain pre-checked software update packages.

It is recommended to audit the real-time activity of camera ports and formed requests, block redundant requests or traffic, use firewalls with verified access instructions for a specific camera model, i.e. use special measures to ensure the encryption of the streams generated by the camera (audiovisual content and service channel) to the information-receiving device. Security control of the cameras can be performed by a separate specialised hardware security attachment connected to the camera via an Ethernet interface, which does not affect the basic functionality of the camera. The function of the security attachment is to provide real-time access control, access monitoring, anomaly detection, camera traffic encryption, and the implementation of a specialised camera network.

ANNEX 1

The following six cameras of different manufacturers were examined: Hikvision DS-2CD2183G0-IU, Dahua IPC-HFW1230-0280B-S1, and Dahua IPC-HDBW2531R-ZS, Xiaomi Mi Home Security Camera 360 1080P, TP-Link Tapo C200, Axis Communications Axis M3044-V View. Risk analysis of the software functionality of these products and the flows created by them and a decomposition study of the hardware part was conducted. During the investigation of the hardware section, a conformity analysis of the chips used in the devices was performed, the circuit-technical structure of the product and the quality of its manufacturing were evaluated. In this investigation, the equipment was dismantled to a point beyond which reassembly would only be possible with the use of precision soldering / desoldering equipment, thus increasing the risk of irreversible damage to microcircuit information due to the high temperature used in the process.

Hikvision and Dahua cameras have been found to have functionality very similar to cameras in the study carried out in May 2020 (Hikvision DS-2CD4C26FWD-AP and Dahua DH-IPC-HFW5231EP-ZE). The Hikvision camera control mobile application Hik-Connect has been updated to HikCentral. Five of the examined cameras are manufactured in China, and one in Sweden (Axis Communications).

Images of the products used in the examination are shown in Figures 1 and 2.

DS-2CD2183G0-IU

IPC-HDBW2531R-ZS

IPC-HFW1230-0280B-S1

Fig. 1. Images of Hikvision and Dahua products used in the examination

Tapo C200

Mi Home Security Camera
360 1080P

Axis M3044-V View

Fig. 2. Images of TP-Link, Xiaomi and Axis Communications products used in the study

The Hikvision Dome Camera DS-2CD2183G0-IU [4] is an outdoor device with an Ambarella S3L-M-B0-RH main processor using an ARM Cortex-A9 core supporting 8 MP resolution, 4K definition, H.265/H.265+/H.264/H.264+ compression technologies for audiovisual content. Memory used in the camera: Samsung K4B4G1646E-BCMA DDR3L 4 Gbit SDRAM random access memory [2] and Toshiba TC58BVG0S3HTA00 type 1 Gb NAND FLASH memory [3]. The manufacturer declares compliance with IP66 and IK10 physical security standards.

The Dahua dome camera IPC-HDBW2531R-ZS [5] is a device for external use with an Ambarella S2LM33 DSP processor supporting H.265+ / H.265 / H.264+ / H.264 audiovisual content compression formats, based on the Linux operating system. The manufacturer declares compliance with IP67 and IK10 physical security standards.

The Dahua Camera IPC-HFW1230-0280B-S1 [6] is an outdoor camera that supports H.265+/H.265/H.264+/H.264 content compression, FullHD definition and 2 MP resolution. The manufacturer declares compliance with the IP67 physical protection standard.

The TP-Link Camera Tapo C200 [7] is an indoor camera with Realtek's RTS3903 processor, XMC's XM25QH64AHIG 64 Mbit SPI FLASH memory, and Realtek's RTL8188FTV WLAN (802.11 b/g/n) controller. The camera supports H.264 audiovisual content compression format. The administration and functionality of the camera is ensured through a mobile application.

The Xiaomi Mi Home Security Camera 360 1080P (MJSXJ02CM) [8] is an indoor camera with MStar's MSC313E image processor that supports H.264 and H.264 audiovisual content

compression formats. The camera uses EON's EN25QH128A serial 128 Mb FLASH memory, which supports SPI, DSPI and QSPI protocols. Mediatek's chip MT7601UN, which supports 802.11 b/g/n standards, was used to implement the WiFi interface.

The dome camera Axis M3044-V View [9] of Axis Communications is an outdoor device with Ambarella S2L-A2-RH processor with ARM Cortex-A9 core, manufactured using 28 nm low power CMOS technology. This processor is capable of processing up to 14 MP images and up to 5M @ 30fps videos. The camera uses Micron memories: MT29F2G08ABAGAH4-IT 1 Gb NAND FLASH memory and two MT41K128M16JT-125 DDR3L 2 Gb SDRAM memories. The camera supports H.264 and VBR/MBR H.264 audiovisual content compression formats.

Indicative prices of the examined cameras: Hikvision DS-2CD2183G0-IU costs EUR 180, Dahua IPC-HDBW2531R-ZS – EUR 270, Dahua IPC-HFW1230-0280B-S1 – EUR 70, TP-Link Tapo C200 – EUR 32, Xiaomi Mi Home Security Camera 360 1080P (MJSXJ02CM) – EUR 33, Axis Communications Axis M3044-V View – EUR 290.

REFERENCES

[1] Report on the Assessment of Cyber Security of Video Surveillance Cameras Supplied in Lithuania. https://www.nksc.lt/doc/biuleteniai/2020-05-27%20Hikvision%20ir%20Dahua%20kameru%20kibernetinio%20saugumo%20vertinimas.pdf
[2] Samsung Memory Documentation https://www.samsung.com/semiconductor/global.semi/file/resource/2017/11/DS_K4B4G1646E-BC_Rev101-0.pdf
[3] Toshiba memory documentation. https://datasheet.lcsc.com/szlcsc/1905191130_TOSHIBA-TC58BVG0S3HTA00_C113406.pdf
[4] Hikvision DS-2CD2183G0-IU Feature Description https://www.hikvision.com/en/products/IP-Products/Network-Cameras/Pro-Series-EasyIP-/DS-2CD2183G0-IU/
[5] Dahua DH-IPC-HDBW2531R-ZS / VFS Documentation. https://www.dahuasecurity.com/asset/upload/product/20180322/DH-IPC-HDBW2531R-ZSVFS_Datasheet_20180202.pdf
[6] Dahua DH-HAC-HFW1230S Documentation. https://www.dahuasecurity.com/asset/upload/product/20180723/DH-HAC-HFW1230S_Datasheet_20180718.pdf
[7] TP-Link Tapo C200 Documentation. https://static.tp-link.com/2020/202001/20200106/Tapo%20C200(EU&US)1.0_Datasheet.pdf
[8] Xiaomi Mi Home Security Camera 360 ° 1080P Camera Documentation. https://i01.appmifile.com/webfile/globalimg/Global_UG/Mi_Ecosystem/Mi_Home_Security_Camera_360_1080P/en_V1.pdf
[9] Axis Communications AXISM3044-V Camera Documentation. https://www.networkwebcams.co.uk/downloads/axis/axis_m3044-v_data-sheet.pdf
[10] infosecurity-magazine.com – Xiaomi Security Camera Shows User Wrong Video Feed. https://www.infosecurity-magazine.com/news/xiaomi-camera-shows-wrong-video/
[11] „Axis products in security scanner audits“. https://www.axis.com/files/tech_notes/technote_axis_products_sec_scanner_audits_en_2007_lo.pdf
[12] Description of the ONVIF Standard. https://www.onvif.org/
[13] xda-developers.com – Google temporarily kills Mi Home integration with Assistant following creepy Xiaomi security camera bug. https://www.xda-developers.com/google-temporarily-kills-xiaomi-mi-home-integration-security-camera-bug/
[14] krebsonsecurity.com – Dahua, Hikvision IoT Devices Under Siege. https://krebsonsecurity.com/2017/03/dahua-hikvision-iot-devices-under-siege/
[15] ipvm.com – Dahua Wiretapping Vulnerability. https://ipvm.com/reports/dahua-audio
[16] Bloomberg – Banned Chinese Security Cameras Are Almost Impossible to Remove. https://www.bloomberg.com/news/articles/2019-07-10/banned-chinese-security-cameras-are-almost-impossible-to-remove
[17] cisa.gov ICS Advisory (ICSA-17-124-02) – https://us-cert.cisa.gov/ics/advisories/ICSA-17-124-02