Tel. +370 706 82 250
E-mail: cert@nksc.lt
https://www.nksc.lt

NATIONAL CYBER SECURITY CENTRE UNDER THE MINISTRY OF NATIONAL DEFENCE REPUBLIC OF LITHUANIA

EXAMINATION FOUND SECURITY RISKS IN HIKVISION AND DAHUA VIDEO SURVEILLANCE CAMERAS

27 May 2020

TLP: WHITE

Remote control of the cameras that could be affected by cyber-attacks, poor password safety solutions, software vulnerabilities, such are a few of the risks found by the National Cyber Security Centre under the Ministry of National Defence (NCSC) thorough the assessment of cyber security of Hikvision and Dahua Chinese manufacturers' video surveillance cameras used in Lithuania.

According to the NCSC assessment, video surveillance cameras of other manufacturers on the market may have the same security gaps, and the identified risks primarily speak of poor management of the IT maintenance.

The National Cyber Security Centre began the video surveillance camera assessment in the beginning of the year, after the national broadcaster LRT published an article about possibly low-security IP cameras that had been blacklisted in the United States of America. Cybersecurity experts conducted the examination of actual video surveillance cameras currently used in practice in Lithuanian institutions, the investigation was carried out in such a manner that peer researchers could repeat the same actions in the same sequence obtaining the same results. The assessment metric was based on the analysis of software functionality, data flow structure, and hardware component decomposition.

The assessment found a number of known cybersecurity gaps in software packages used in the IP cameras that are listed and publicly available in the Common

Tel. +370 706 82 250
E-mail: cert@nksc.lt
https://www.nksc.lt

Vulnerabilities and Exposures (CVE) database. Those gaps present a real risk of cyber-attacks, such as DoS or insertion of malware. Cameras do not have automatic update function, while the update infrastructure is held on China's and Russia's servers.

The research also observed poor password protection mechanisms that were used: the IP cameras did user authentication transmission without encryption, only through HTTP with outdated MD5 algorithm. Therefore, the password value can be intercepted, password decoded, and eventually used for unlawful login which allows to take over the camera stream, activate or deactivate camera functions in real time (face recognition, sound recording, etc.), or shut down the camera.

It was also identified that Hik-Connect mobile app for Hikvision camera remote control connects to servers in China, Thailand, Singapore, and Ireland, as well as registers SIM card IMSI and ICCID numbers, as well as mobile device IMEI numbers.

According to the poll carried out by the NCSC, 57 public sector institutions are using the Chinese Hikvision and Dahua video surveillance cameras in Lithuania. Institutions are urged to familiarise with the recommendations on the management of the risks identified in the report of NCSC.

The NCSC recommends Hikvision and Dahua camera users to isolate the cameras in a dedicated physical or logical network without connection to service, local or public Internet networks. It is also advised to organise download of updates from remote servers located in NATO or European Union countries. Real-time audit of port activity is recommended on a regular basis in order to prevent unnecessary communications, as well as to white-list required functionalities only.

Generally, it is recommended to include a requirement for the supplier to provide the cameras with the most recent manufacturer software updates in which identified security gaps and vulnerabilities would be repaired into technical specifications when conducting public procurement. The supplier should also arrange downloads of software updates from NATO and EU-based servers, cameras provided by the supplier should have only the functionalities listed in technical specifications and excess functionalities should be deactivated.