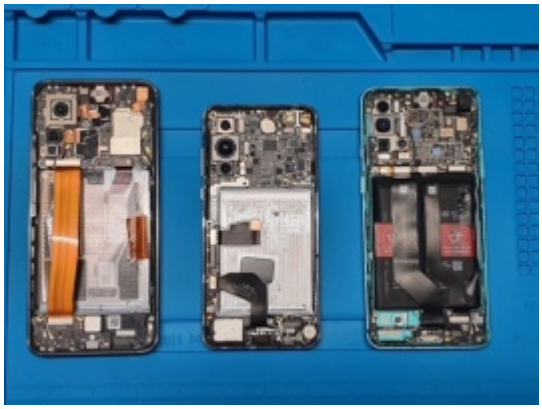
Ministry of National Defence Republic of Lithuania :: News » News Releases

News Releases



The National Cyber Security Centre under Ministry of National Defence conducted a cyber security assessment of 5G smart phones made by Chinese manufacturers and supplied in Lithuania: Huawei P40 5G , Xiaomi Mi 10T 5G, OnePlus 8T 5G.

"The investigation was initiated to ensure a safe use of 5G devices and software in Lithuania that are sold in our country. For that purpose, three Chinese manufacturers that have been supplying 5G mobile devices to Lithuanian consumers since last year and are identified as somewhat risky by the international community were selected," says Vice Minister of National Defence Margiris Abukevičius.

The investigation has found four substantive cybersecurity risks: two concern inbuilt apps, one – personal data security, and one more – possible clash with the freedom of speech requirement. Three of the cybersecurity risks have been found in Xiaomi cell phone, one in Huawei, and no cybersecurity vulnerabilities have been identified in OnePlus.

Risks from manufacturer apps

Assessment of a Huawei 5G cell phone has found that AppGallery, the official app store installed by the manufacturer, automatically redirects to their-party e-shops if it does not include what the user is looking for. Part of the apps offered in such e-shops are recognized by antivirus programmes malware or infected.

The investigation also attributed cybersecurity risks to Mi Browser, the web browser on Xiaomi-manufactured cell phones. It uses not only Google Analytics as other browsers but also Chinese Sensor Data, which collects and periodically sends out data on as many as 61 functionalities regarding user activities on the device.

„In our view, this is excess information collection on user activities. Another risk factor is the fact that the abundant statistical data is sent to Xiaomi servers in third countries that do not observe General Data Protection regulation via an encrypted channel and is also stored there," says Dr. Tautvydas Bakšys, head of Innovation and Training Division of the National Cyber Security Centre under Ministry of National Defence.

Possible infringements on your freedom of speech

Assessment of a Xiaomi device has revealed a technical functionality that could censor the content of downloaded material. Several apps on the smart phone, including Mi Browser, are periodically downloading a list of banned keywords from the manufacturer. If the content the user is downloading contains keywords from the list, it is automatically blocked.

At the time when the investigation was conducted, the list included 449 keywords and keyword combinations in Chinese characters, for example, free Tibet, America's voice, democratic movement, Long Live the Democratic Taiwan, etc.

"We have found that the content filter functionality is disabled in the Xiaomi cell phones supplied to Lithuania and does not carry out the content censorship activity, however, the censored keyword lists are still periodically updated. The device is technically enabled to activate the functionality remotely at any time without the user's permission and to begin censoring the downloaded content. We do not rule out that the banned keyword list can be drawn using Latin, not just Chinese characters," T. Bakšys says.

Personal data security risk

The personal data security risk was found in a Xiaomi device, specifically, Xiaomi Cloud service. Activation of the service requires sending an enciphered SMS message to register, it is not saved on the device.

"The investigators were not able to read the encrypted message and verify its content. The automated messaging and content concealed by the manufacturer poses a potential threat to personal data security, as it enables collection and transfer of unidentifiable personal data to servers in third countries," says T. Bakšys.

Why the particular manufacturers

Chinese manufacturers Huawei, Xiaomi and OnePlus introduced fifth generation, 5G, mobile communication-supporting smart phones into the Lithuanian market in 2020. According to the international Vulnerabilities and Exposures (https://cve.mitre.org) database, cybersecurity risks have been identified on devices from all the mentioned manufacturers in the recent four years. 9 vulnerabilities concerning personal data security were found in Xiaomi products, 144 vulnerabilities , most of which concerned interference with device functionalities, were identified on Huawei products, and one vulnerability was found on OnePulse products, its concerned a third country app that sent SMS messages even when the device was locked.

The full text of Cyber security assessment publicly available at www.nksc.lt/en/reports.html

For the Media

Today, September 21, at 1400 hrs, Vice Minister of National Defence Margiris Abukevičius and Dr. Tautvydas Bakšys, Head of Innovation and Training Division of the National Cyber Security Centre under Ministry of National Defence, will be available for comments. Please register until 1200 at vis@kam.lt, +370 614 29091, MoD Strategic Communications Department Please give your name and surname, media outlet, contacts - cell phone no., e-mail address.

Freelance reporters and foreign media representatives will need accreditation given by the MoD Strategic Communication and Public Relations Department.

Photo credit: National Cyber Security Centre under Ministry of National Defence

Back

Comment

Ministry of National Defense Republic of Lithuania has a right to delete inappropriate comments.

Name

email

Comment text

Security code

Submit

URL: https://kam.lt/en/news_1098/current_issues/things_your_smart_phone_does_without_your_awareness_investigation_into_three_china-made_5g_devices.html