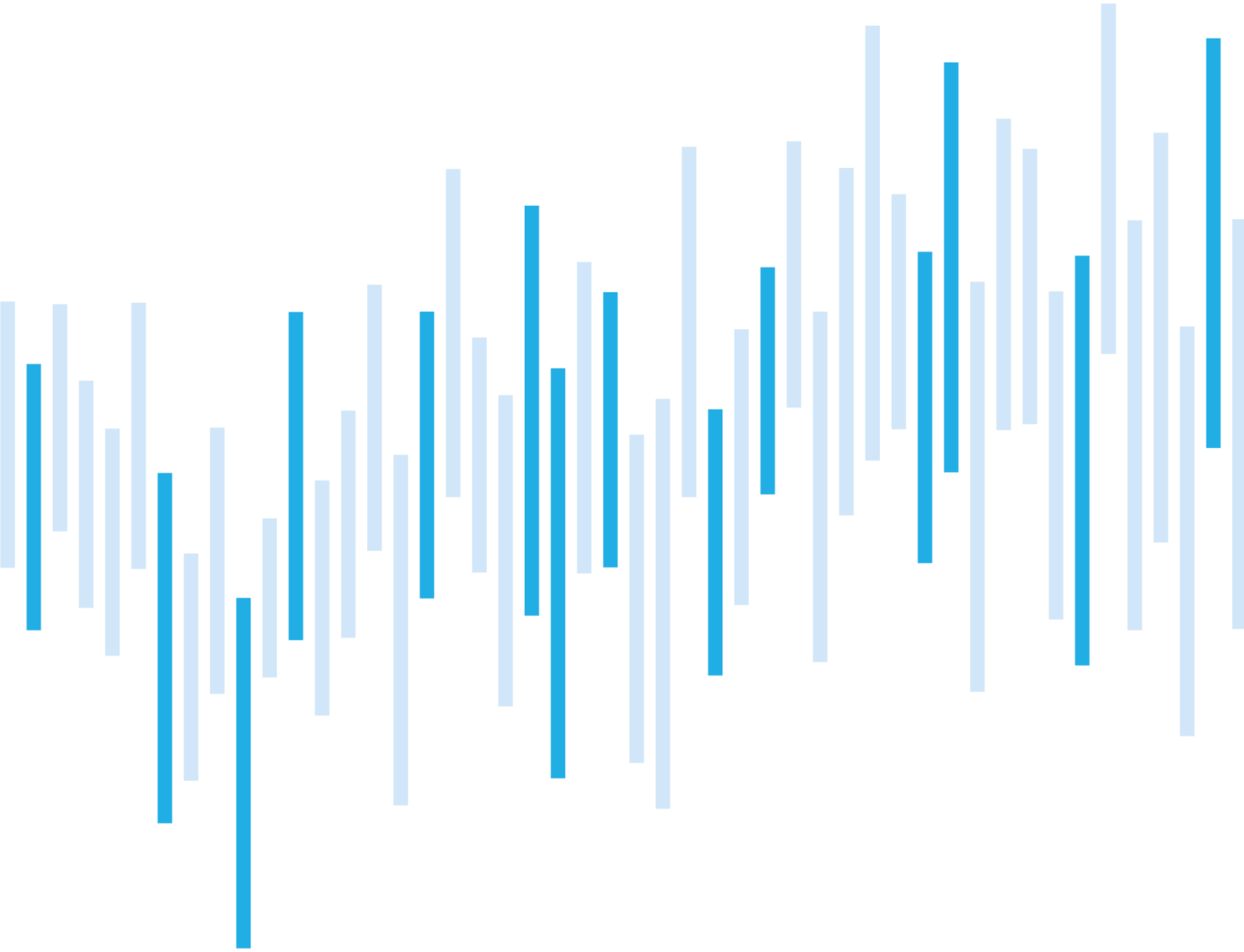
CYBER INCIDENTS FROM THE NÚKIB'S PERSPECTIVE

DECEMBER 2021



Národní úřad
pro kybernetickou
a informační bezpečnost

Summary of the month

In December, both global and Czech cyber scenes were shocked by the publishing of the CVE-2021-44228 vulnerability, also known as Log4Shell. Log4Shell is a critical vulnerability, which potentially affects hundreds of millions of systems. The code for its exploitation is freely available, and an attacker does not even need to have advanced technical skills to be able to execute it. Attackers can use the code to gather credentials, exfiltrate data or install other malicious codes, including ransomware.

Contrary to the concerns, exploitations of this vulnerability did not gain significant representations in December's cyber incidents. Only two out of fifteen incidents addressed by NÚKIB were linked to Log4Shell. However, it is likely (55-70%) that the Log4Shell exploitation is still in its infancy and the number of incidents will increase in the coming months. APT groups are gradually adding the Log4Shell exploit code to their toolboxes. Ransomware groups are buying access to systems vulnerable to Log4Shell. Consequently, Log4Shell is likely to open doors to many organisations, including the Czech ones.

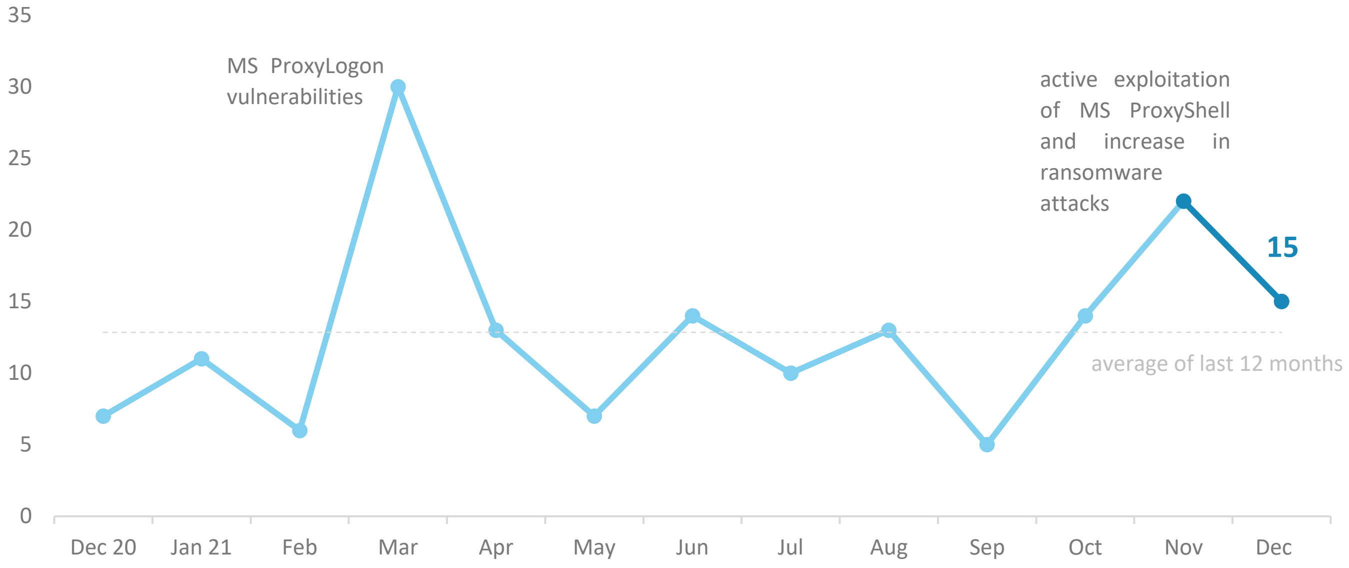
Table of contents

The following report summarises the events of the month. The data, information, and conclusions contained herein are primarily based on cyber incidents reported to NÚKIB. If the report contains information from open sources in some sections, the origin of this information is always stated.

You can send comments and suggestions for improving the report to the address komunikace@nukib.cz.

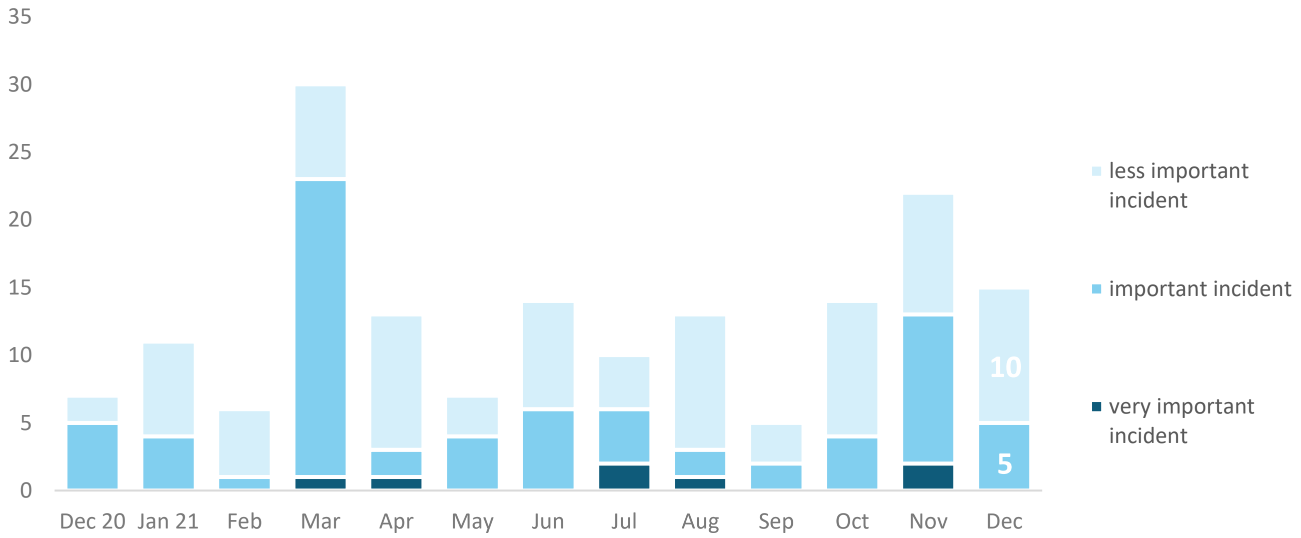
Number of cyber incidents reported to NÚKIB

Compared to November, the number of cyber incidents fell by seven in December. Despite the new Log4Shell vulnerability, which affects many computer programmes and applications, the number of incidents was lower than we feared after its publication.[1]



Severity of the handled cyber incidents[2]

In December, NÚKIB did not address any very important incident incidents and classified one-third of all incidents as important. Although the latter limited operations of the attacked organisations in some cases, the organisations quickly managed to resolve the situation and restore the services.

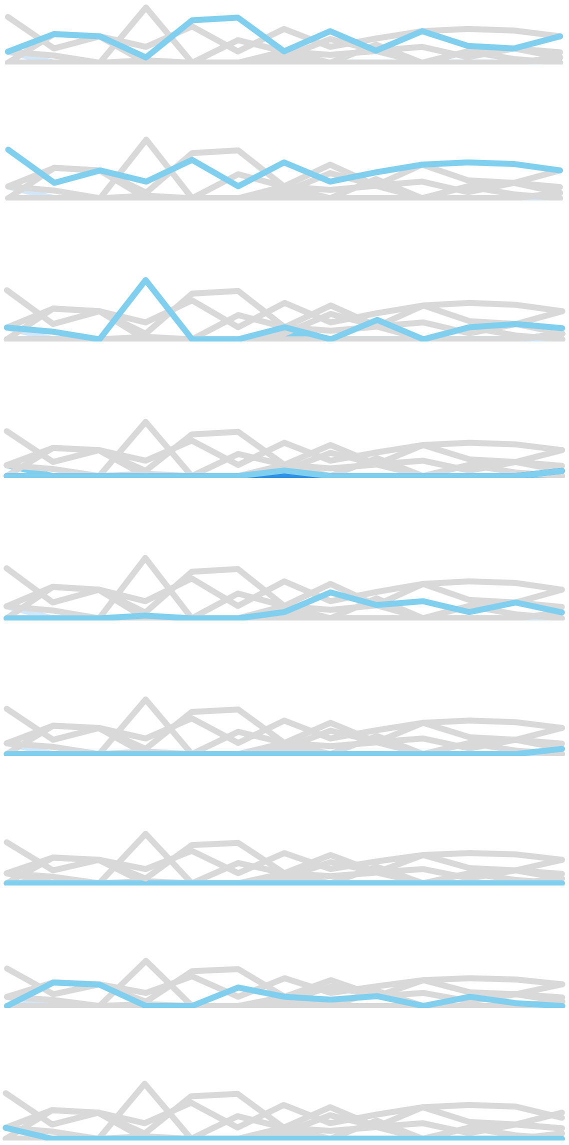


[1] Six incidents were reported to NÚKIB by obligated persons according to the Cyber Security Act. The remaining nine incidents were reported by entities that do not fall under this law.
[2] NÚKIB determines the severity of cyber incidents on the basis of Decree No. 82/2018 Coll. and internal methodology.

Classification of the incidents reported to NÚKIB[3]

As in previous months, malicious code and incidents resulting in service unavailability are at the top. The availability incidents included a DDoS attack, a technical error, and ransomware, which resulted into limited operations of two of the attacked organisations, whose backup solutions were insufficient. The malicious code category included ransomware, too, but the victim's functional backups prevented it from affecting the service availability. This category further included detections of malware C2 servers and one incident related to the Log4Shell vulnerability exploitation by attackers who installed a cryptominer on their victim's web server (for more information about the Log4Shell vulnerability and related incidents, see p. 6).

	December 2020	December 2021
Malicious code such as a virus, worm, Trojan horse or spyware	14 %	**33 %**
Availability such as disruption in availability caused by a DoS/DDoS attack or sabotage	58 %	**33 %**
Intrusion such as compromising an application or user account	14 %	**13 %**
Intrusion attempt such as an attempt to abuse vulnerabilities or login attempt	0 %	**7 %**
Information content security such as unauthorised access to data, unauthorised change of information	0 %	**7 %**
Other	0 %	**7 %**
Abusive content such as spam, cyberbullying or improper content	0 %	0 %
Fraud such as phishing, identity theft or unauthorised use of ICT	0 %	0 %
Information Gathering such as scanning, sniffing or social engineering	14 %	0 %



[3] The cyber incident classification is based on the ENISA taxonomy: Reference Incident Classification Taxonomy — ENISA (europa.eu)

December trends in cyber security from the perspective of NÚKIB [4]

Phishing, spear-phishing, and social engineering

Unlike in November, when four incidents related to the ProxyShell vulnerability were closely associated with phishing, NÚKIB only dealt with one such case in December involving unknown attackers who compromised an e-mail server of a Czech state organisation and sent fraudulent messages from it in German.

Two Czech public organisations picked on phishing attempts, but no compromising was found.

Malware

Emotet operators, who returned to the global and Czech cyber scene in November, continued their campaign. NÚKIB detected two Czech organisations compromised by Emotet, which used their infrastructures as its C2 servers to control further attacks.

NÚKIB also discovered the Dridex C2 server, which primarily targets bank details of its victims, in another Czech organisation.

Vulnerabilities

In December, the whole world reverberated with the newly released vulnerability “Log4Shell”, identified as CVE-2021-44228, which may affect hundreds of millions of devices, enabling attackers to gain full control over systems of organisations with minimum efforts. Having considered the severity of the vulnerability, NÚKIB has issued a reactive measure. For more information, see page 6.

Furthermore, the MS ProxyShell campaign went on in the Czech Republic in December. It involved the incident described above in the section on phishing.

Ransomware

Compared to the preceding month, the number of ransomware attacks has decreased. NÚKIB only dealt with three incidents linked to ransomware in December as compared with six such incidents in November. One of the attacked organisations had functional backups and managed to restore its infrastructure operation in no time. The other two organisations did not have fully functioning backups and the ransomware somewhat limited their operations. The ransomware that attacked Czech organisations in December was Phobos, BlackCat, and Hive.

Attacks on availability

Just like in November, only one DDoS attack occurred in December’s incidents. It took place in three waves, each of which caused approximately a 15-minute loss of the attacked organisation’s service.

[4] The development illustrated by the arrow is evaluated in relation to the previous month.

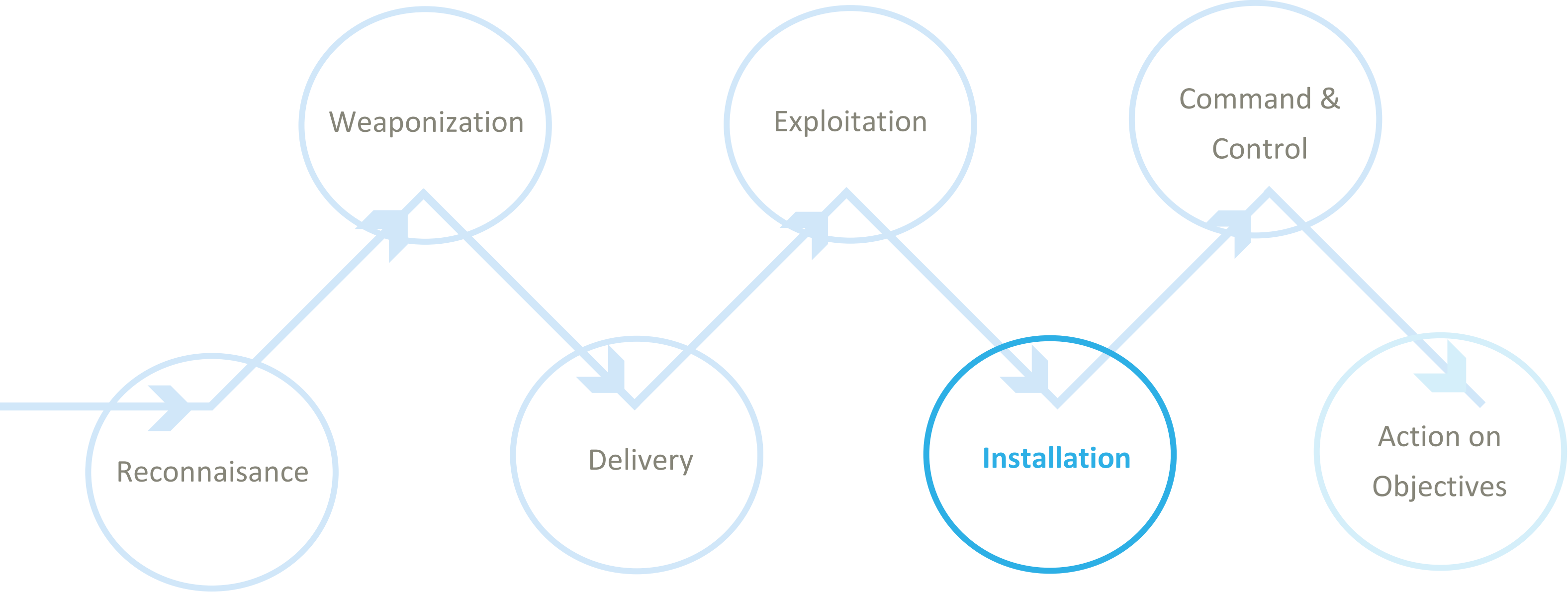
The most used technique of the month: Process Injection

NÚKIB also evaluates cyber incidents based on the MITRE ATT&CK framework, which serves as an overview of known techniques and tactics used in cyber attacks. On its basis, NÚKIB determines, among other things, the frequency of the use of techniques.

The most frequent technique in December incidents was "Data Encrypted for Impact", which we described in the July report. To avoid repetitions in the reports, this chapter discusses the "Process Injection" technique, which was the second most widely used in December. It occurred in the incidents associated with Log4Shell, during which attackers uploaded a code in the Log4j logging tool.

> **Process Injection** is a method of adding malicious code to the legitimate processes in the victim's system. When a user launches a tool to view running processes, they will only see legitimate processes. Thereby, attackers want to impair detecting their movements to remain unnoticed in the victim's system. Examples of Process Injection include uploading a malicious code into the memory process of the browser used by the victim, shared libraries or any other process running in the victim's system.
>
> **MITRE ID: T1055**
>
> **Mitigation:** Some tools for detection and reaction to attacks on terminal equipment (such as EDR – Endpoint Detection & Response) can be configured to intercept the commonly known steps that attackers take when using the Process Injection technique.

The representation of "Process Injection" in a kill chain shows at which point attackers use the technique. The incidents addressed by NÚKIB had this point in Installation.



Focused on the threat: Log4Shell

What is Log4Shell?

CVE-2021-44228, a vulnerability also known as Log4Shell, was published on 9 December 2021. This vulnerability was found in the Log4j logging tool. Modern software solutions are complex programmes developed by large teams. Rather than being written line by line, they are put together using existing “building blocks”. One of such blocks is Log4j. Software developers add it to their products to be able to monitor what is going on in the products and address potential issues. Most of the present-day software solutions can log, and some of them use Log4j to do so. There are probably hundreds of millions of systems, applications and services that use the Log4j tool and may be vulnerable.

Log4shell is a very severe vulnerability. The exploit code is freely available and is very simple. Using it does not require advanced technical skills, yet it enables attackers to perform almost anything. Attackers can use the exploit code to gain access to the systems of their victims, steal their credentials, data or install other malicious codes, including ransomware.

What is the global situation?

Massive worldwide exploitation of the vulnerability began a few days after its publishing. Most attacks monitored by the Microsoft Threat Intelligence Center (MSTIC) have groups running cryptominers or DDoS botnets behind them. Nevertheless, the MSTIC has already confirmed that some groups sell access to networks of organisations they have gained by exploiting Log4Shell to groups operating on the ransomware-as-a-service (RaaS) basis. According to MSTIC, actors backed by China, Iran, and North Korea have also started to add the Log4Shell exploit codes to their toolboxes. It is, therefore, likely that the number of more significant attacks by APT and ransomware groups will be growing in the following months.

What is the situation in the Czech Republic?

In December, NÚKIB addressed two cyber incidents associated with Log4Shell. The first organisation intercepted the Log4Shell exploitation when the attacker was trying to install a remote-control tool in the organisation’s system. In the other case, the attackers exploited the vulnerability to install a cryptominer in the webserver of the attacked organisation. Given the widespread nature of Log4Shell, it is almost certain that there are more affected organisations than NÚKIB currently registers.

2 **cyber incidents**

5 % **of provably vulnerable organisations**

NÚKIB does not know the exact number of vulnerable systems located in the Czech Republic. NÚKIB can make deduction based on scans performed on the basis of the reactive measure issued. The number of vulnerable machines cannot be determined using Shodan because the Log4Shell vulnerability scan is so intrusive that it would in fact become an incident. When the reactive measure was released, dozens of organisations turned to NÚKIB asking for scanning of their systems. Five per cent of those organisations was provably vulnerable to Log4Shell. However, it does not mean that the systems of the remaining 95% were all right. Most scans performed by NÚKIB were stopped anti-scanning technologies. Third parties hence cannot simply determine whether there are any vulnerable systems in the infrastructures of the organisations. A sophisticated attacker would be able to circumvent such a measure, but it is effective against wide-scale scans by which attackers try to detect vulnerable systems with the least possible effort. Moreover, NÚKIB only scanned perimeters of organisations, but there may be many more vulnerable machines inside their infrastructures.

Recommendations

Individuals

Log4j is incorporated in tools and services that everyone uses daily. The best individuals can do is to continuously update all their devices and applications. Developers have been repairing them one by one since the publishing of the vulnerability.

Organisations

NÚKIB recommends organisations to follow the steps to secure their systems provided in the reactive measure of 15 December 2021.

Probability Terms Used

Probability terms and expression of their percentage values:

Term	Probability
Almost certain	90–100 %
Highly likely	75–85 %
Likely	55–70 %
Realistic probability	25–50 %
Unlikely	15–20 %
Highly unlikely	0–10 %

Conditions for the Use of Information

The information provided shall be used in accordance with the Traffic Light Protocol methodology (available at the website www.nukib.cz). The information is marked with a flag, which sets out conditions for the use of the information. The following flags are specified that indicate the nature of the information and the conditions for its use:

Colour	Conditions
TLP:RED	Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.
TLP:AMBER	Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.
TLP:GREEN	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.
TLP:WHITE	Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.