ICT Security Newsletter 04/2021

rittmeyer
BRUGG

Vulnerabilities in Log4j (also called Log4Shell)

The German Federal Office for Information Security (BSI) has declared the highest level of alert. The Swiss National Cyber Security Center (NCSC) also takes the situation extremely seriously and warns that critical infrastructure could be attacked. The Java library Log4j is a component used in many Java applications. It is not foreseeable how many Internet services will be affected.

What is at stake?

On December 9, 2021 it became known that a critical vulnerability exists in the widely used Java library Log4j. The threat level of the vulnerability (CVE-2021-44228) is rated “high”. Affected is Log4j from version 2.0-beta9 to 2.14.1. The manufacturer has released version 2.15.0 at short notice, which closes the gap.

Increasingly, widespread scans are being observed that search for vulnerable applications with the previously unknown gap. If the vulnerability is found, hackers can use it to execute their own code on affected systems and take them over completely.

The NCSC warns strongly that the vulnerability could be used to attack critical infrastructure in Switzerland. So far, no such reports have been received. In the attacks observed by the NCSC, hackers attempted to install malware such as “Mirai”, “Kinsing”, and “Tsunami”. Kinsing is a crypto miner, the Mirai and Tsunami botnets are mostly used for DDoS attacks.

What is the threat situation at my facility?

The vulnerable Java library is used in numerous Java applications and is therefore very widespread. Although a security update is already available for the actual library, the applications based on it must also be adapted.

The following Rittmeyer core systems are not affected :

- **RITOP**
- **RIFLEX**
- **RISOURCE**
- **RITUNE**
- **RICITY**
- **Rittmeyer instrumentation**

Furthermore, the following third-party components used by Rittmeyer are not affected:

- **Windows™ operating system**
- **SonicWall firewall**
- **NetExtender VPN connection**
- **Westermo**
- **Moxa**
- **Siemens PLC**

In order to do all that is necessary, organizations must first gain an overview of which of their systems and software solutions use Log4j.

The NCSC has already taken active measures. After the patch was released, national operators of critical infrastructure were immediately called upon to apply it as soon as possible. In addition, one has started to warn the operators of Log4j instances that can be directly reached via the Internet. Even if a particular solution is vulnerable in principle, this does not automatically mean that attackers can actually exploit a vulnerability.

How can I protect my facility?

There is a security update for the affected Java library Log4j. Security specialists are working feverishly to identify vulnerable systems and close gaps. The NCSC calls on all companies and organizations to immediately patch all systems that are connected to the Internet. For internal systems, they should do so as soon as possible thereafter. Systems that cannot be patched should be disconnected from the Internet or, at the very least, emergency measures recommended by vendors should be taken.

How Rittmeyer can help you:

Update Service
With the Update Service, Rittmeyer takes care of testing and installing patches and hotfixes. Especially for the firewall and the operating system it is recommended to install all available security updates at regular intervals to close known security gaps.

Vulnerability scan
A security specialist scans your system with special software to detect existing vulnerabilities and close them promptly.

If you feel unsafe, or are interested in one of our ICT security services, contact your Rittmeyer representative directly.

Rittmeyer AG
6341 Baar, Switzerland
P +41 41 767 10 00, F +41 41 767 10 70
security@rittmeyer.com, www.rittmeyer.com/itsecurity