Product Security Bulletin

Important Information - Please Read and Keep

Subject: Log4j Security Vulnerabilities (Log4Shell)

Date: 2021-12-15 (last update)
Originator: Timo Kosig

Background

Security researchers at the Alibaba Cloud Security Team have discovered a new critical vulnerability in the Log4j java logging framework (link). Versions of Log4j affected include any version with version number >=2.0-beta9 and < 2.16.0. The Log4j logging framework is very popular and often used by Java applications to facilitate logging. The vulnerability has been assigned the vulnerability identifier CVE-2021-44228 and has since been dubbed "Log4Shell" by security researchers.

Since Log4j is widely used and the vulnerability trivially exploitable (with exploits already available on the internet), there are already reports in the media of massive exploitation of the vulnerability to attack systems.

In light of discovery of the Log4Shell vulnerability, security researchers have tested if previous versions of Log4j are vulnerable as well. While they found that Log4j 1.x does not contain the Log4Shell vulnerability, they discovered a separate vulnerability in Log4j 1.x. This vulnerability has been assigned the vulnerability identifier CVE-2021-4104.

What both vulnerabilities have in common

CVE-2021-44228 and CVE-2021-4104 are different in terms of their attack vectors, although both vulnerabilities can be used to accomplish remote code execution (RCE) using special strings known as JNDI requests.

For both vulnerabilities, the JNDI request could contain a reference to an LDAP server, which the vulnerable Log4j versions would (unless specifically disabled by configuration) use to send a query to said LDAP server in order substitute the text string with the response from the LDAP server. This mechanism can be exploited to fetch a specified Java class from a remote source and deserialize it, executing the class's code in the process which compromises the system.

What Log4Shell (CVE-2021-44228) does

For CVE-2021-44228, an attacker would try to get the system under attack to log JNDI requests, e.g. by inserting the request into the username field of a login form with the assumption that the username is logged for each authentication attempt. This could be carried out on local or remote systems running the affected Log4j versions.

Due to the trivial nature of the exploit, the possible consequences and the remote attack vector, CVE-2021-44228 has received the highest possible CVSS 3.1 (Common Vulnerability Scoring System) base score of **10.0 (Critical)**.

What CVE-2021-4101 does

The flaw behind CVE-2021-4104 is in the use of JMSAppender within the Apache Log4j library. Applications running version 1.2.x with JMSAppender enabled and with JMSAppender set to allow JNDI requests run the risk of an attacker performing an exploit that can lead to remote code execution. In different scenario, an attacker with write access to the Log4j configuration could set the JMSAppender to their own JMS Broker. This would allow the attacker to send JNDI requests to the application.

CVE-2021-4104 received a CVSS 3.1 base score to **6.6 (Medium)** due to the local attack vector and JMSAppender not being enabled by default.

Response

Affected Vyaire Products

Log4Shell (CVE-2021-44228)

Vyaire's products **do not make use** of the Log4j library versions that is vulnerable to the Log4Shell vulnerability and are therefore **not vulnerable** to any exploits.

CVE-2021-4101

Vyaire Respiratory Diagnostics' SentryConnect solution, which is utilized to connect SentrySuite™ solutions to hospital information systems, utilizes Mirth Connect for integration purposes. Mirth Connect utilizes an older version of Log4j that is **potentially vulnerable to CVE-2021-4104**, but **not vulnerable to CVE-2021-44228**. Mirth Connect does not make use of the vulnerable JMSAppender in its Log4j configuration by default.

Mirth Connect does have updates planned in their roadmap to move to a newer and non-vulnerable version of Log4j. Vyaire will monitor their development, and will align internally to use a new Mirth Connect version for future SentryConnect versions.

How Vyaire Is Responding

Vyaire is monitoring the ongoing situation around the recent disclosure of the Log4j vulnerabilities.

Vyaire will continue to evaluate information as it becomes available to determine whether any of Vyaire's products are impacted.

Mitigations & Compensating Controls

Log4Shell (CVE-2021-44228)

Vyaire products are not affected by Log4Shell, therefore no mitigations for Log4Shell are required for Vyaire products.

CVE-2021-4101

Vyaire recommends to apply the following mitigations and compensating controls:

- Review access controls to ensure only authorized personnel has write-level access to Log4j configuration files.

Vyaire is currently investigating the possibility of removing the vulnerable JMSAppender class from the Log4j JAR-package file in-place or replacing the JAR package file with a version that does not contain the JMSAppender class. This bulletin will be updated once a recommendation is available.

Generic controls

- Ensure your data has been backed up and stored according to your individual process and that your disaster recovery procedures are in place.
- Update your anti-virus and malware protection, where available.

For product or site-specific concerns, contact your Vyaire service representative.

For more information on Vyaire's proactive approach to product security and vulnerability management, contact us at productsecurity@vyaire.com or visit www.vyaire.com/product-security.

Timo Kosig
timo.kosig@vyaire.com
Product Security Leader
Vyaire Medical