Puzzel Log4j Critical Incident Report 2021-12-14

Zero-Day Exploit (CVE-2021-44228) Targeting Popular Java Library

Tor-Ståle Hansen
CISO Puzzel

This document explains the implications and how the incident has affected Puzzel and our products and services. This is the first documentation, future documents may add further insights and knowledge, but this is what we know so far.

General information

On Friday morning, Puzzel received notification from the Norwegian National Cyber Security Centre (NCSC) and NorCERT, about a critical vulnerability in a popular Java library called "Log4j". At the time of receiving these reports, the vulnerability apparently has been exploited by threat actors "in the wild" and no patch was available to fix the vulnerability (Zero-day exploit).

Log4j is a popular Java library developed and maintained by the Apache foundation. The library is widely adopted and used in many commercial and open-source software products as a logging framework for Java.

The vulnerability (CVE-2021-44228) is critical, as it can be exploited from remote by any adversary to executed arbitrary code (remote code execution – RCE). The criticality of the vulnerability has a score of 10 (out of 10) in the common vulnerability scoring system (CVSS) which outlines how severe the vulnerability is.

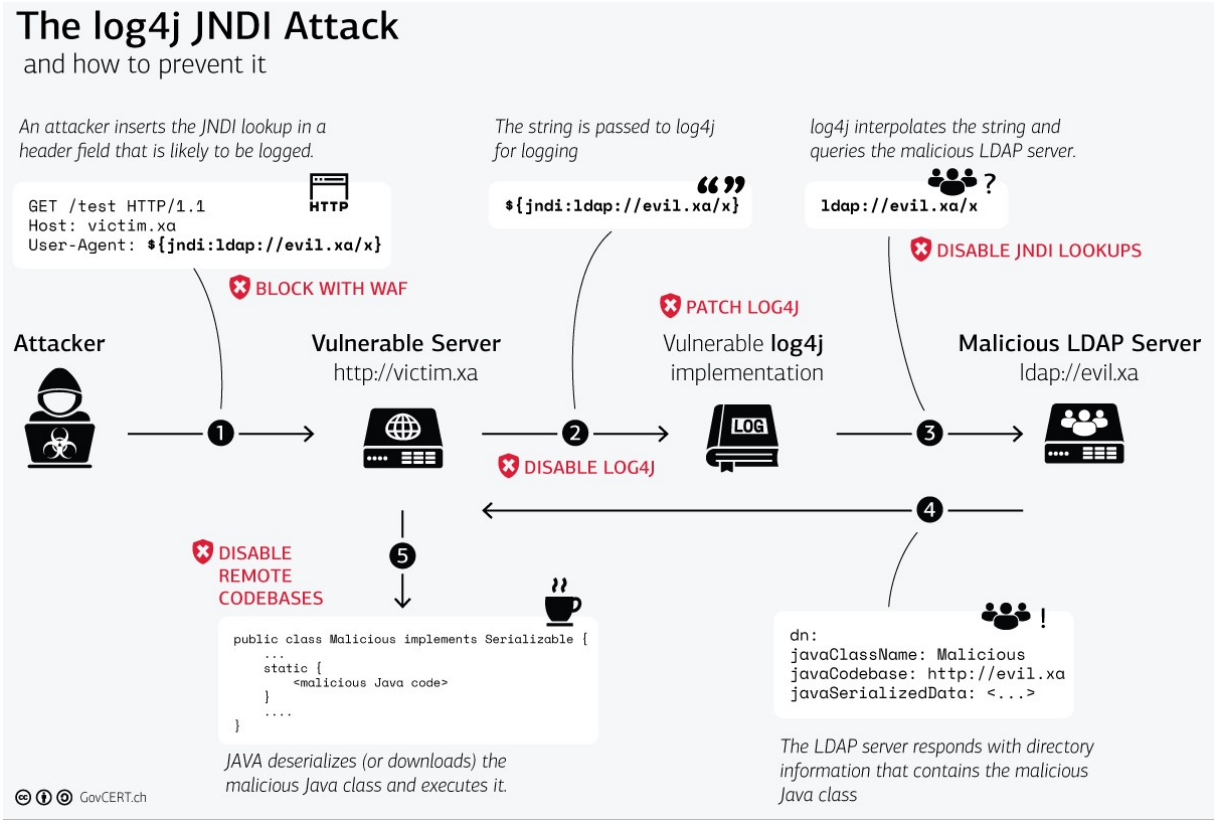
The vulnerability results from how log messages are being handled by the log4j processor. If an attacker sends a specially crafted message, this may result in loading an external code class or message lookup and the execution of that code, leading to a situation that is known as Remote Code Execution (RCE).

The criticality is not only related to log services, but a broader spectrum attack surface. Sun Microsystems released JNDI (Java Naming and Directory Interface API on March 10 1997. In their press release the functionality and then the adversary opportunities are clearly explained:

> "Any Java application that needs to access information about users, machines, networks, and services can utilize JNDI. User information includes security credentials, phone numbers, electronic and postal mail addresses, and application preferences. Machine information includes network addresses, machine configurations, etc. In addition, any Java application (examples include printers, calendars, and networked file systems) that needs to either export objects or access objects exported by other applications and services will benefit from JNDI."
>
> SUN Microsystems, Press Release of March 10, 1997

Puzzel Log4j Critical Incident Report 2021-12-14

Synopsis – what we understand



While certain products may be vulnerable, it doesn't necessary mean that the vulnerability can be successfully exploited as this depends on several pre- and postconditions such as the JVM being used, the actual configuration, etc. Any version of log4j between versions 2.0 and 2.14.1 are affected.

External recognized recommended mitigations

- Get an overview of systems and software using log4j in your environment.
- Apply the corresponding security patches for internet facing software / devices immediately
- Apply the corresponding security patches for internal software / devices at your earliest convenience.
- If patching is not possible for whatever reason, it is strongly recommend isolating the system from the Internet.

What are the general plausible implications?

CVE-2021-44228 enables attackers to perform remote code execution, which means they can run any code and access all data on the affected machine. It also allows them to delete or encrypt files and hold them for ransom. Any function the impacted asset can do, attackers can do as well with the exploit. This means anything that uses a vulnerable version of Log4j to log user-controlled data can be attacked.

Puzzel Log4j Critical Incident Report 2021-12-14

Beside Log4j, the full spectrum opportunity though JNDI API services over LDAP, DNS, NIS, NDS, RMI and COBRA, mean that the full exploit (in theory) is possible through any Java application that can establish full access to information about users, machines, networks, and services can utilize JNDI.

User information includes security credentials, phone numbers, electronic and postal mail addresses, and application preferences. Machine information includes network addresses, machine configurations, etc. In addition, any Java application (examples include printers, calendars, and networked file systems) that needs to either export objects or access objects exported by other applications and services will benefit from JNDI.

How Puzzel have reacted to this incident

Short summery and status update: of the last days after NSM NCSC announced the security vulnerability.

Incoming information	
2021-12-10 09:39	[NCSC-NO#21375915] [NCSC Alert] Critical Vulnerability in Apache Log4j
2021-12-10 12:50	[NCSC-EN # 21551146] [NCSC Alert] Updated Apache Log4j2 Critical Vulnerability Alert
2021-12-10 22:28	[NCSC-EN # XXXXX] [NCSC Alert] IMPORTANT - Update: Critical Vulnerability in Apache Log4j *Information is exempt from public access, cf. the Public Access to Information Act § 21
2021-12-11 22:28	[NCSC-EN # 21825943] [NCSC Alert] Extended Update for Apache log4j CVE-2021-44228 *Information is exempt from public access, cf. the Public Access to Information Act § 21
Puzzel actions	
2021-12-10 10:00-11:13	CISO does initial investigations, and contact internal SME's and mgmt. for further investigations on internal products and services.
2021-12-11	Initial investigations conclude that no Puzzel products or services that are internet facing are affected by this threat.
2021-12-13 15:00	Further internal investigations unveil that a third party service is affected by the vulnerability from CVE-2021-44228. The investigation team discission was to block this service until the vendor have patched the service.
2021-12-17	Puzzel have initiated further mitigations with regards to the parallel CVE-2021-45046. Puzzel is in contact with vendors for their reports on this latest CVE. The CSSV score on this is minor 3.7, compared to critical 10.0 of the base CVE for this Log4j incident.
IOC's (Indication of Compromise)	
2021-12-14	No indications

- END OF DOCUMENT -

Puzzel Log4j Critical Incident Report 2021-12-14