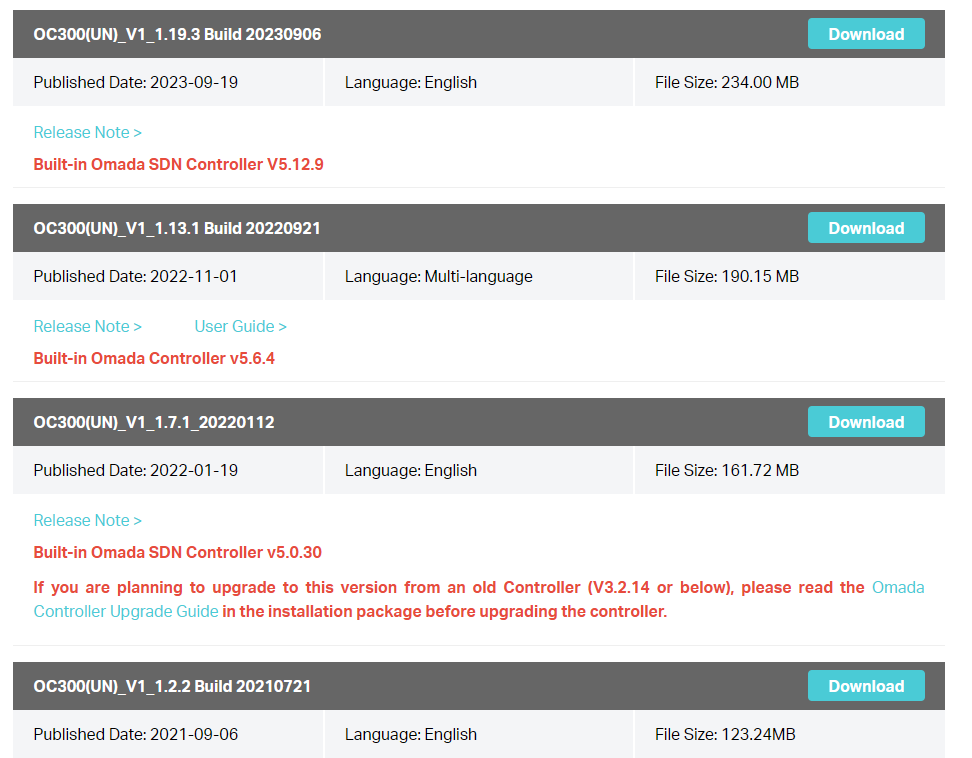
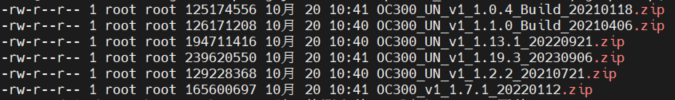
1. 从网站https://www.tp-link.com/no/support/download/oc300/v1/?app=web#Firmware可以下载OC300的固件



下载存储到本地：



1. 使用长亭科技的Log4j2 漏洞检测工具检测

根据<https://log4j2-detector.chaitin.cn/>所述，可以线上与线下检测，这里采用线下检测

$ ./log4j2\_local\_scanner\_linux\_amd64.v3 --root /home/zhang/Desktop/Log4j2/待测文件/tp-link\_oc3000/固件/OC300\_UN\_v1\_1.1.0\_Build\_20210406.zip



没有检测出来，这跟包的结构有关。

继续分析：

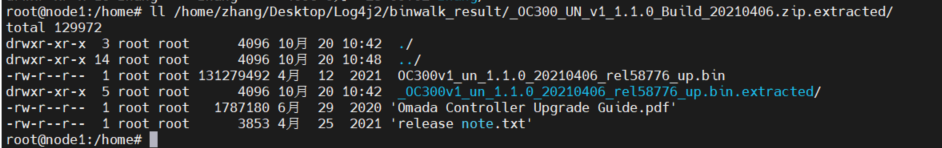
使用binwalk解包：

binwalk --run-as=root -Me -d 8 -r OC300\_UN\_v1\_1.1.0\_Build\_20210406.zip -C /home/zhang/Desktop/Log4j2/binwalk\_result/ > OC300\_UN\_v1\_1.1.0\_Build\_20210406.zip.binwalk.log

解包日志：

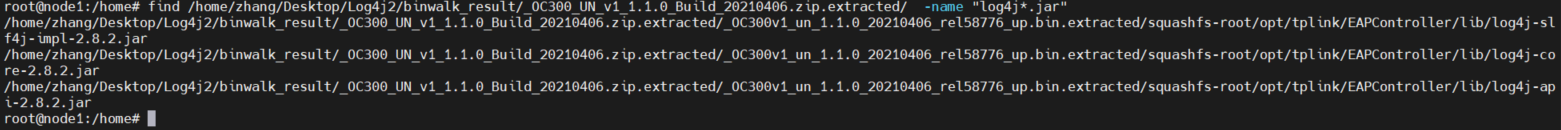


解包结果：



在解包路径下查找有无logj-\*.jar包：

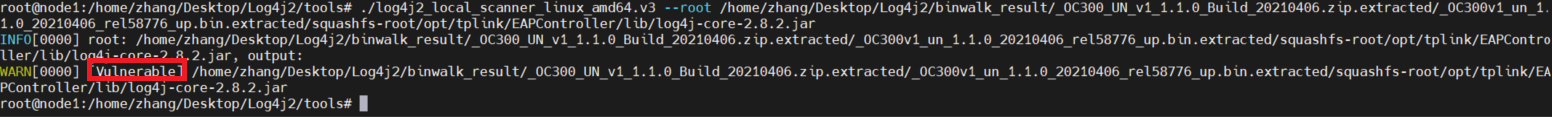
$ find /home/zhang/Desktop/Log4j2/binwalk\_result/\_OC300\_UN\_v1\_1.1.0\_Build\_20210406.zip.extracted/ -name "log4j\*.jar"



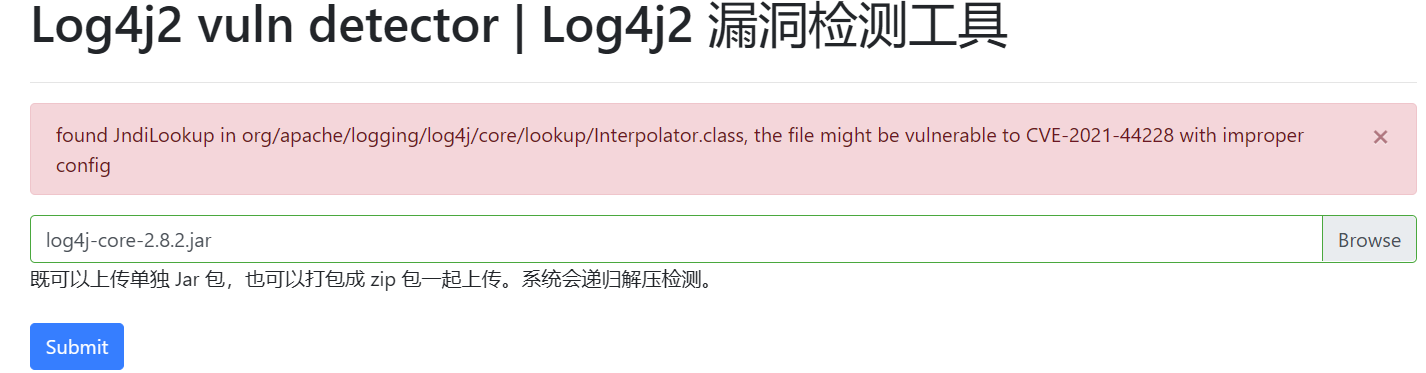
可以看到，存在log4j-core-2.8.2.jar，位于/home/zhang/Desktop/Log4j2/binwalk\_result/\_OC300\_UN\_v1\_1.1.0\_Build\_20210406.zip.extracted/\_OC300v1\_un\_1.1.0\_20210406\_rel58776\_up.bin.extracted/squashfs-root/opt/tplink/EAPController/lib/log4j-core-2.8.2.jar。

根据Log4j漏洞影响范围，可以推断log4j-core-2.8.2.jar包含Log4j CVE-2021-44228漏洞，但还需要进一步确认。

使用长亭科技的Log4j漏洞检测工具检测：



线上检测更直白，结果如下：



log4j-core-2.8.2.jar是由解包后的bin文件OC300v1\_un\_1.1.0\_20210406\_rel58776\_up.bin（Hxd可以查到）引入的。对于这种直接检测是检测不出的，需要进行解包再分析。

1. 编写yara规则检测

Yara规则如下：



部分yara规则如下：

rule log4j\_memory

{

meta:

author = "BI.ZONE"

version = "0.12"

description = "Process memory signatures for Log4j"

license = "Just do whatever you want"

strings:

$s\_1 = "\\log4j\\core\\" wide

$s\_2 = "\\apache\\logging\\log4j\\" wide

$s\_3 = "/apache/logging/log4j/" ascii

$s\_4 = "/log4j/core/config/" ascii

$s\_5 = "org.apache.logging.log4j." ascii

$s\_6 = "org.apache.log4j" ascii

$s\_7 = "org/apache/log4j/" ascii

$s\_8 = "log4j:message" ascii

$a\_1 = "Log4j appears to be running in a Servlet environment" ascii

$a\_2 = "this tool is superseded by the annotation processor included in log4j-core" ascii

$a\_3 = "Error parsing Log4j schema" ascii

$a\_4 = "org.apache.logging.log4j2:type=%s,component=Loggers,name=%s,subtype=RingBuffer" ascii

$a\_5 = "log4j:ERROR" ascii

$a\_6 = "log4j error:" ascii

$a\_7 = "$log4j$spi$ErrorHandler" ascii

$this\_rule = "we\_dont\_want\_to\_detect\_this\_rule\_in\_memory" ascii

condition:

2 of ($s\_\*) or 1 of ($a\_\*) and (not $this\_rule)

}

rule RegularLog4j

{

meta:

author = "zq"

description = "Other components include Log4j"

strings:

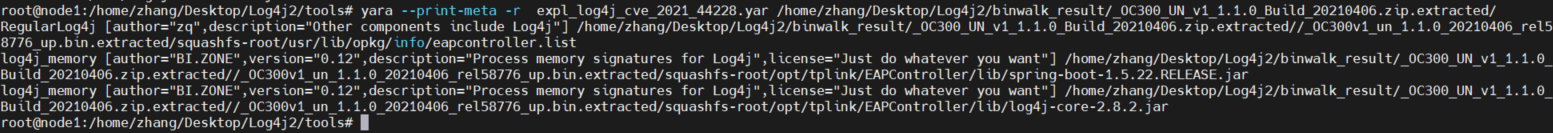
$re1 = /log4j-core-2\.\b([0-9]|1[0-5])\b[\.\d]\*\.jar/

condition:

$re1

}

使用yara检测：检测出了



1. 分析到这，可以确定固件OC300\_UN\_v1\_1.1.0\_Build\_20210406.zip存在log4j CVE-2021-44228漏洞。