登录

Apache Synapse远程命令执行漏洞分析—【CVE-2017-15708】

大又甜的西瓜 / 2017-12-20 10:15:00 / 浏览数 3110 技术文章 技术文章 顶(0) 踩(0)

0x01. 漏洞概述

近日，CVE更新了一个 Apache Synapse的严重安全漏洞。该漏洞存在于版本低于3.0.1的 Synapse产品上，允许攻击者在运行有 Apache Synapse的目标系统上远程执行任意代码。目前，国家信息安全漏洞共享平台（CNVD）已对该漏洞进行了收录（CNVD-2017-36700，对应CVE编号:CVE-2017-15708）。

0x02. 漏洞分析

从官网上下载 Apache Synapse2.1的源码，IDE打开载入。在依赖包列表中，可以看到 Commons-collections3.1的身影。该包的存在使得 Apache Synapse上有关序列化/反序列化的操作变得十分危险。因此此时要触发 Synapse中的反序列化远程命令执行漏洞，只需确认 Synapse中存在反序列化的相关操作即可。

通过对比启动 Synapse前后的端口开放情况，可以明显的看到，Synapse 启动后会对 1099 这个端口进行监听。默认情况下，该端口是 Java RMI 服务的默认监听端口。而 RMI 正是 100% 基于序列化操作的。如果该端口上运行的恰好是 RMI 服务，那么触发漏洞的两个条件至此就全部满足了。

为了不让分析停留在猜测上，我们跟踪一下程序的执行过程。通过搜索关键字 `main` ，在排除一些官方 demo 造成的干扰后，找到程序的入口函数在 `SynapseServer` 类中。

在 Synapse 开发人员友好的注释帮助下，忽略和排除掉一些诸如"启动失败"之类的无关代码。因为要证明的是 Synapse 在启动过程中执行过序列化有关的代码，因此在跟踪过程中，对一些异常情况可以先忽略不理，直接看执行成功这一种情况的流程即可。依照这个原则，跟随程序执行依次来 `ServerManager` 类中的`start()`方法以及 `SynapseController` 的 `start()`方法上。 其中，由于 `Axis2SynapseController` 是 `SynapseController` 接口的实现类，所以直接跟踪 `Axis2SynapseContrllor` 的`start()`方法即可。 `Axis2SynapseContrllor` 的`start()`方法如下：

继续略过无关代码后，直接来到 `Axis2SynapseContrllor` 的 `start()` 方法的尾部。从官方的注释来看，如果启动顺利，到这里JMX已经配置并启动成功了，准备输出相关信息。但在输出前做了一个对象是否创建成功的判断，所以这里我们跟进

以关键字 `jmxAdapter` 搜索文档，在当前类 `Axis2SynapseContrllor` 中可以发现 `jmxAdapter`对象的实例化代码如下：

继续跟进后来到 `JmxAdapter` 类的 `start()` 方法下。容易在方法中找到 "RMI" 的关键字，跟进进去，最后在 `RMIRegistryController` 类中看到了看到了熟悉的注册 "RMI" 服务的代码：

可见， Apache Synapse 在启动的过程中，确实使用了 RMI 的方法实现了 JMX ，而 Synapse 的源码中又使用了存在脆弱性的 Commons-Collections 依赖包，因此通过向运行有 RMI 服务的 Synapse 服务器发送精心构造过的序列化数据，攻击者便可以达到在远程服务器上执行任意命令的目的。

0x03. 受影响情况分析

开启了全程使用序列化数据传输的Java RMI服务是触发该漏洞的条件之一，该服务使用的1099默认端口在全网的开放情况如下(未确认风险)：

该服务的端口在全国的开放情况如下(未确认风险)：

0x04. 时间线

- 2017年12月10日 更新漏洞报告
- 2017年12月11日 创建CVE
- 2017年12月15日 昊天实验室发布漏洞分析

0x05. 漏洞验证与修复

我们提供了一个验证工具验证主机是否存在漏洞：https://github.com/hucheat/APacheSynapseSimplePOC

- 在远程服务器上弹出计算器验证：
- 反弹 MSF会话：

修复建议

- 目前Apache已发布修复该漏洞的 Synapse 新版本3.0.1，请到官网下载并更新新版本。

相关资料

[1] http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-15708

[2] http://www.securityfocus.com/bid/102154

[3] http://www.cnvd.org.cn/flaw/show/CNVD-2017-36700

[4] http://synapse.apache.org/download/3.0.1/download.cgi

[5] https://github.com/hucheat/APacheSynapseSimplePOC

点击收藏 | 0 关注 | 0

上一篇：CISP报考相关信息 下一篇：有没有大牛分享下学习思路。。。

1. 0 条回复
   - 动动手指，沙发就是你的了！

登录 后跟帖

先知社区

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