2019-04-17-Confluence路径遍历漏洞

Confluence -路径遍历漏洞 -CVE-2019-3398

主题	CVE-2019-3398 - 在下载附件资源时存在路径遍历漏洞
公告发布日期	17 Apr 2019
涉及产品	• Confluence Server • Confluence Data Center
Confluence Server版本影响	• 2.0.0 <= version < 6.6.13 • 6.7.0 <= version < 6.12.4 • 6.13.0 <= version < 6.13.4 • 6.14.0 <= version < 6.14.3 • 6.15.0 <= version < 6.15.2 • All 2.x.x versions • All 3.x.x versions • All 4.x.x versions • All 5.x.x versions • All 6.0.x versions • All 6.1.x versions • All 6.2.x versions • All 6.3.x versions • All 6.4.x versions • All 6.5.x versions • All 6.6.x versions **before** 6.6.13 • All 6.7.x versions • All 6.8.x versions • All 6.9.x versions • All 6.10.x versions • All 6.11.x versions • All 6.12.x versions **before**6.12.4 • All 6.13.x versions**before**6.13.4 • All 6.14.x versions**before**6.14.3 • All 6.15.x versions**before**6.15.2
修复版本	• 6.6.13 • 6.12.4 • 6.13.4 • 6.14.3 • 6.15.2

脆弱性概述

本公告披露了Confluence Server和Confluence数据中心版本2.0.0中引入的严重性安全漏洞。Confluence Server和数据中心的版本从6.6.13之前的2.0.0（6.6.x的固定版本）、6.12.4之前的6.7.0（6.12.x的固定版本）、6.13.4之前的6.13.0（6.13.x的固定版本）、6.14.3之前的6.14.0（6.14.x的固定版本）和6.15.2之前的6.15.0开始受此漏洞影响。

Atlassian云实例不受本页所述问题的影响。

将Confluence Server和/或数据中心升级到6.6.13或6.12.4或6.13.4或6.14.3或6.15.2版本的客户不受影响

下载并安装了以下版本的Confluence Server或数据中心的客户会受到影响：

- All 2.x.x versions
- All 3.x.x versions
- All 4.x.x versions
- All 5.x.x versions
- All 6.0.x versions
- All 6.1.x versions
- All 6.2.x versions
- All 6.3.x versions
- All 6.4.x versions
- All 6.5.x versions
- All 6.6.x versions **before** 6.6.13
- All 6.7.x versions

- All 6.8.x versions
- All 6.9.x versions
- All 6.10.x versions
- All 6.11.x versions
- All 6.12.x versions **before**6.12.4
- All 6.13.x versions**before**6.13.4
- All 6.14.x versions**before**6.14.3
- All 6.15.x versions**before**6.15.2

请立即升级Confluence服务器或数据中心安装以修复此漏洞：

DownloadAllAttachments资源中的路径遍历-CVE-2019-3398

严重程度

Atlassian根据我们在Atlassian严重性级别中发布的级别，将此漏洞的严重性级别评定为“关键”。该量表允许我们将严重程度分为临界、高、中或低。

这是我们的评估，您应该评估它对您自己的IT环境的适用性。

描述

Confluence Server和数据中心在DownloadAllAttachments资源中存在路径遍历漏洞。**有权向页面和/或博客添加附件，或创建新空间或个人空间的远程攻击者，或对空间具有“管理”权限的远程攻击者**，可以利用此路径遍历漏洞将文件写入任意位置，从而在运行易受攻击版本Confluence的系统上执行远程代码。服务器或数据中心。

确认

找到这个漏洞的功劳归IT中心的J_nis Krusts所有。

修复

可以根据以方法来进行修改

- 安装Confluence Server and Data Center versions 6.15.2版本，可以从 https://www.atlassian.com/software/confluence/download/ 下载
- 安装Confluence Server and Data Center versions 6.6.13, 6.12.4, 6.13.4 and 6.14.3 ，可以从 https://www.atlassian.com/software/confluence/download-archives

我们需要做什么

我们建议更新到最新版本. 对一进了新版本的功能描述 ，可以参见Release Notes.

如果我们不能升级到 6.15.2或者更高版本

(1) 我们可以升级到以下对应的版本中，这几个版本我们已经做了修复

If you have feature version	then upgrade to bugfix version:
6.12.0, 6.12.1, 6.12.2, 6.12.3	6.12.4
6.13.0, 6.13.1, 6.13.2, 6.13.3	6.13.4
6.14.0, 6.14.1, 6.14.2	6.14.3

(2) 如果我们使用了企业版本,我们可以升级到企业版本相就的最新版本.

如果我们使用以下版本	那么可以升级到以下版本:
6.6.0, 6.6.1, 6.6.2, 6.6.3, 6.6.4, 6.6.5, 6.6.6, 6.6.7, 6.6.8, 6.6.9, 6.6.10, 6.6.11, 6.6.12	6.6.13
6.13.0, 6.13.1, 6.13.2, 6.13.3	6.13.4

(3) 我们使用了旧的版本，即在2018年10月4号之前发布的版本，企业版本在2017年4月4号之前的版本，我们可以升级到相就的最新版本If

缓解

如果我们不能马上进行升级，我们可以临时通过以下方法来解决。

sssssss<base-url>/<context-path>/pages/downloadallattachments.action的方法.关掉会不能使用此页面下载任何的附件，也不能使用附件宏。

按以下步骤操作:

1. 停掉Confluence.
2. ss<install-directory>/conf/server.xmlss

3. 在 <Host> 增加以下配置t:

```
<Context path="/pages/downloadallattachments.action" docBase="" >
    <Valapp className="org.apache.catalina.valapps.RemoteAddrValapp" deny="*" />
</Context>
```

如果我们的Confluence路径为/wiki，配置就为以下格式

```
<Context path="/wiki/pages/downloadallattachments.action" docBase="" >
    <Valapp className="org.apache.catalina.valapps.RemoteAddrValapp" deny="*" />
</Context>
```

4. 保存文件然后重新启动Confluence

验证:

1. 浏览页面s.
2. 在页面 ••• 进入到附件，点击下载全部附件.

此时将不能访问，页面为404.