Atlassian Confluence 远程代码执行漏洞(CVE-2021-26084)

一、漏洞信息

2021 年 8 月 26 日，Atlassian 官方发布了关于 Atlassian Confluence 远程代码执行漏洞的风险通告，漏洞编号为 CVE-2021-26084，Atlassian 将此漏洞的级别评为“严重”；Atlassian Confluence 产品存在 OGNL 注入漏洞，允许经过身份验证的攻击者（在某些情况下未经身份验证的用户）在 Confluence Server 或 Data Center 实例上执行任意代码。

二、漏洞危害

Atlassian Confluence 产品存在 OGNL 注入漏洞，允许经过身份验证的攻击者（在某些情况下未经身份验证的用户）在 Confluence Server 或 Data Center 实例上执行任意代码。

三、影响范围

Confluence Server 和 Confluence Data Center：

- 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
- 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
- All 6.13.x versions < 6.13.23
- All 6.14.x versions
- All 6.15.x versions
- All 7.0.x versions
- All 7.1.x versions
- All 7.2.x versions
- All 7.3.x versions
- All 7.4.x versions < 7.4.11
- All 7.5.x versions
- All 7.6.x versions
- All 7.7.x versions
- All 7.8.x versions
- All 7.9.x versions
- All 7.10.x versions
- All 7.11.x versions < 7.11.6
- All 7.12.x versions < 7.12.5

四、修复方案

Atlassian 官方已经发布了解决此漏洞的软件更新，建议受影响用户尽快升级到安全版本：

已修复版本:6.13.23、7.4.11、7.11.6、7.12.5 和 7.13.0

安装和更新方式可以参考以下链接：
https://www.atlassian.com/software/confluence/download-archives

若无法及时进行升级，建议采用官方的临时措施进行防御：

Linux 环境下:

1.关闭 Confluence。

2.下载 cve-2021-26084-update.sh 到 Confluence Linux 服务器，配置安装目录和脚本运行权限之后，执行更新脚本进行安全更新。

3.更新成功重启 Confluence

Windows 环境下:

1.关闭 Confluence。

2.下载 cve-2021-26084-update.ps1 Powershell 脚本到 Confluence Windows 服务器。配置安装目录和并以管理员权限执行更新脚本进行安全更新。

3.更新成功重启 Confluence

具体更新步骤可参考官方通告：

https://confluence.atlassian.com/doc/confluence-security-advisory-2021-08-25-1077906215.html

五、参考资料

https://confluence.atlassian.com/doc/confluence-security-advisory-2021-08-25-1077906215.html

https://confluence.atlassian.com/doc/files/1077906215/1077916296/2/1629936383093/cve-2021-26084-update.sh

https://confluence.atlassian.com/doc/files/1077906215/1077916298/2/1629936382985/cve-2021-26084-update.ps1