

2021-04-09-jQuery安装漏洞

漏洞说明

系列版本等于或低于1.12的jQuery，和2.x系列版本等于或低于2.2的jQuery，过滤用户输入数据所使用的正则表达式存在缺陷，可能导致LOCATION.HASH跨站漏洞。

Atlassian的相关产品，JIRA, Confluence使用了jquery. 2.2.4版本，可以使用jQuery安全版本来进行替换。

漏洞官方修复介绍：<http://bugs.jquery.com/ticket/9521>

风险级别

中危

JIRA漏洞修复

- 可以在安装目录下atlassian-jira\static-assets的目录下找到：jquery-min.js 将其替换掉（最好同名）
- 在安装目录下：atlassian-jira\WEB-INF\atlassian-bundled-plugins，找到：jquery-2.2.4.7.jar 文件，需要对这里包的文件进行修改（此jar包里的内容版本较早，注意兼容性）
 - 找到jquery-min.js，jquery.js 将其替换掉（最好同名）
 - 如遇不想同名，需要修改atlassian-plugin.xml中文件的name="jquery web-resource" 中的定义

对文件替换掉后，重新启动JIRA

Confluence漏洞修复

- 在安装目录下：confluence-jira\WEB-INF\atlassian-bundled-plugins，找到：jquery-2.2.4.7.jar 文件，需要对这里包的文件进行修改（此jar包里的内容版本较早，注意兼容性）
 - 找到jquery-min.js，jquery.js 将其替换掉（最好同名）
 - 如遇不想同名，需要修改atlassian-plugin.xml中文件的name="jQuery - Core library"中的定义

对文件替换掉后，重新启动Confluence

说明

jquery不同的版本可能在接口上有所差异，如何进行兼容性保障系统稳定，可以查看jquery的升级说明，并对对产品进行严格测试。

有可能所使用的插件包含有jquery，具体可以联系插件厂商咨询如何修复。

如果使用的为DataCenter版本，并进行了集群部署，在多个结点中都需要进行相同操作