2022-07-20关于CVE-2020-14179漏洞解决办法

描述

通过 /secure/QueryComponent!Default.jspa 端点暴露敏感数据

受影响的 Atlassian Jira Server 和 Data Center 版本允许未经身份验证的远程攻击者通过 /secure/QueryComponent!Default.jspa 端点中的信息泄露漏洞查看自定义字段名称和自定义 SLA 名称。

影响版本

- version < 8.5.8
- 8.6.0 ≤ version < 8.11.1

修复版本

- 8.5.8
- 8.11.1 及以上，包括 8.13.x

解决方案

修复版本中解决办法：

禁用站点范围匿名访问的暗功能，

- 添加暗功能“**public.access.disabled**”

禁用成功，在上述修复版本中，端点现在将为匿名用户返回 401

- 添加新添加的暗功能“**com.atlassian.jira.plugin.issuenavigator.anonymousPreventCfData.enabled**”

禁用成功，

1. 将返回 200，但是只有在未经过身份验证时，输出才会从响应中过滤掉所有自定义字段
2. ❗ 打开“com.atlassian.jira.plugin.issuenavigator.anonymousPreventCfData.enabled”标志的副作用是在问题搜索的基本模式下（https://confluence.atlassian.com/jirasoftwareserver/basic-searching-939938708.html）不会有任何可用于匿名使用的自定义字段 + 应该会显示“您尚未登录，因此您不能在基本搜索中使用自定义字段。登录或切换到高级搜索。”的警告。
   高级模式应该可以正常工作（https://confluence.atlassian.com/jirasoftwareserver/advanced-searching-939938733.html）

注：如何进入匿名访问暗功能：以管理员身份登录并转到[BASE-URL]/secure/SiteDarkFeatures!default.jspa

影响版本解决办法：

server版本

1. 编辑文件 JIRA_INSTALL/atlassian-jira/WEB-INF/urlrewrite.xml
2. 在最后 </rule> 行的正下方（但在 </urlrewrite> 行之前）插入一条新规则：

```
    <rule>
        <from>(?s)/QueryComponent!.*\.jspa</from>
        <condition type= "session-attribute" name= "seraph_defaultauthenticator_user"  operator = "notequal"
 >.+</condition>
        <set type= "status" >403</set>
        <to> null </to>
    </rule>
```

3. 重启Jira

datacenter版本，每个节点都修改一下，并重启