

2019-08-12-JIRA中的SSRF漏洞-CVE-2019-8451

漏洞说明

版本8.4.0之前的Jira中的/plugins/servlet/gadgets/makeRequest资源允许远程攻击者通过服务器端请求伪造（SSRF）漏洞访问内部网络资源的内容，该漏洞是由Jira中的Whitelist类中的逻辑错误造成的。

在调用/plugins/servlet/gadgets/makeRequest地址时，允许远程攻击都通过服务器端请求伪造（SSRF）漏洞来访问内网资源，比如漏洞加上某一特定请求头，无需求登录即可执行服务端的服务器命令

/plugins/servlet/gadgets/makeRequest?url=http://10.10.10.1:8080@baidu.com

影响版本

7.6.9, 8.1.0, 8.0.2

修复版本

8.4.0, 7.6.17, 7.13.9

修复

可以升级到8.4版本及后续版本

也可以下载新的安装包(8.6.713)