Workspace是否涉及Apache shiro 权限绕过漏洞CVE-2023-34478

戴丽丽 2024-08-08 发表

漏洞相关信息

漏洞编号： CVE-2023-34478

漏洞名称： Apache shiro 权限绕过漏洞

产品型号及版本： E2004

漏洞描述

Shiro 身份认证绕过漏洞(CVE-2023-34478)

Apache Shiro是一个强大且易用的Java安全框架，执行身份验证、授权、密码学和会话管理。使用Shiro的易于理解的API，您可以快速、轻松地获得任何应用程序，从最小的移动应用程序到最大的网络和企业应用程序。

Apache Shiro存在身份认证绕过漏洞，当与基于非规范化请求路由请求的 API 或其他 Web 框架一起使用时，可能会容易受到路径遍历攻击，导致身份验证绕过。将 Apache Shrio 升级到 1.12.0、2.0.0-alpha-3 及以上版本，下载地址：https://github.com/apache/shiro

漏洞解决方案

```
/var/lib/vdi/ssv/BOOT-INF/lib/shiro-cache-1.10.0.jar
/var/lib/vdi/ssv/BOOT-INF/lib/shiro-event-1.10.0.jar
/var/lib/vdi/ssv/BOOT-INF/lib/shiro-core-1.10.0.jar
/var/lib/vdi/ssv/BOOT-INF/lib/shiro-crypto-cipher-1.10.0.jar
/var/lib/vdi/ssv/BOOT-INF/lib/shiro-spring-1.10.0.jar
/var/lib/vdi/ssv/BOOT-INF/lib/shiro-crypto-core-1.10.0.jar
/var/lib/vdi/ssv/BOOT-INF/lib/shiro-quartz-1.10.0.jar
/var/lib/vdi/ssv/BOOT-INF/lib/shiro-web-1.10.0.jar
/var/lib/vdi/ssv/BOOT-INF/lib/shiro-lang-1.10.0.jar
/var/lib/vdi/ssv/BOOT-INF/lib/shiro-ehcache-1.10.0.jar
/var/lib/vdi/ssv/BOOT-INF/lib/shiro-config-ogdl-1.10.0.jar
/var/lib/vdi/ssv/BOOT-INF/lib/shiro-crypto-hash-1.10.0.jar
/var/lib/vdi/ssv/BOOT-INF/lib/shiro-config-core-1.10.0.jar
[root@cvknode2 ssv]#
```

环境中shiro-web版本信息是1.10.0，经分析在非springframework特定场景下可能存在权限绕过的可能，ws使用的springframework框架。

后续欧拉分支也会升级shiro版本。