

知 Apache Shiro身份认证绕过漏洞(CVE-2022-32532)

刘琪 2022-07-14 发表

漏洞相关信息

漏洞编号: CVE-2022-32532

漏洞名称: Apache Shiro身份认证绕过漏洞

产品型号及版本: CAS CloudOS Workspace UIS ONEStor DBaaS MQS 绿洲应用开发平台 DE 绿洲融合集成平台 绿洲数据运营 AIOS

漏洞描述

Apache Shiro 是一个强大且易用的开源 Java 安全框架, 可用于身份验证、授权、加密和会话管理。通过 Shiro 易于理解的 API, 您可以快速轻松地应用其来保护任何应用程序, 从最小的移动应用程序到最大的 web 和企业应用程序。在 Apache Shiro 中存在身份认证绕过漏洞, 源于 RegexRequestMatcher 中正则表达式处理的特性, 导致可能某些需要认证的 Servlet 被绕过。

漏洞名称	Apache Shiro 身份认证绕过漏洞		
公开时间	2022-06-28	更新时间	2022-06-29
CVE 编号	CVE-2022-32532	其他编号	QVD-2022-10156
威胁类型	身份认证绕过	技术类型	授权不当
厂商	Apache	产品	Shiro
风险等级			
奇安信 CERT 风险评级		风险等级	
中危		蓝色 (一般事件)	
现时威胁状态			
POC 状态	EXP 状态	在野利用状态	技术细节状态
已发现	未发现	未发现	已公开
漏洞描述	当 Apache Shiro 中使用 RegexRequestMatcher 进行权限配置, 且规则中使用带点号的正则表达式时, 未经授权的远程攻击者可通过构造恶意数据包绕过身份认证, 导致配置的权限验证失效。		
影响版本	Apache Shiro < 1.9.1		

漏洞解决方案

CAS:不涉及

CloudOS:不涉及

UIS: 不涉及

ONEStor: 不涉及

Workspace: ssv组件使用了1.3.2版本的apache shiro, 规避方法: systemctl stop ssv、system disable ssv。预计解决此漏洞版本: E1012P06

CloudOS MQS: 不涉及

DBaaS: 不涉及

绿洲应用开发平台: 不涉及

绿洲融合集成平台、绿洲数据运营、AIOS: 不涉及

DE: 数据工厂涉及, 如有用到数据工厂, 请联系400确认解决方案。

