OpenClaw WebSocket 共享令牌权限提升漏洞

2026 年 3 月 17 日

一、漏洞概要

漏洞名称	**OpenClaw WebSocket 共享令牌权限提升漏洞**
发布时间	**2026 年 3 月 17 日**
组件名称	**OpenClaw**
影响范围	**OpenClaw ≤ 2026.3.11**
漏洞类型	权限提升
利用条件	**1、用户认证：需要用户认证** **2、前置条件：默认配置** **3、触发方式：远程**
综合评价	**<综合评定利用难度>:复杂,需要有普通用户权限。** **<综合评定威胁等级>：高危，可造成权限提升。**
官方解决方案	已发布

二、漏洞分析

2.1 组件介绍

OpenClaw 是 github 上的开源个人 AI 代理项目，通过 WhatsApp、Telegram、Discord 等聊天工具交互，支持本地/云 LLM，具备自主执行能力（如浏览器控制、设备操作、邮件/文件处理、语音对话）。用来打造常驻本地、能真正干活的个人 AI 助手，用于日常自动化、生产力提升和开发者任务。

2.2 漏洞描述

2026 年 3 月 17 日，深瞳漏洞实验室监测到一则 OpenClaw 组件存在权限提升漏洞的信息，漏洞威胁等级：高危。

OpenClaw 在使用共享令牌或密码进行 WebSocket 连接认证时，服务端未对客户端自行提交的权限作用域做校验与限制，直接信任并采纳客户端声明的高权限，导致持有普通共享令牌或密码的用户可非法声明管理员权限，实现权限提升。

三、影响范围

目前受影响的 OpenClaw 版本：

OpenClaw ≤ 2026.3.11

四、解决方案

4.1 修复建议

1、官方修复建议

官方已发布最新版本修复该漏洞，建议受影响用户将 OpenClaw 更新到 2026.3.12 及以上版本。

下载链接：https://github.com/openclaw/openclaw

2、临时修复建议

- 关闭未使用的功能模块，减少潜在攻击入口。
- 遵循最小权限原则，严控各类敏感操作权限范围。
- 非必要不暴露服务到公网，限制访问源为可信范围。
- 定期更新系统及各类组件至安全版本，及时修补已知隐患。

4.2 深信服解决方案

1、风险资产发现

支持对 OpenClaw 的主动检测，可批量检出业务场景中该事件的受影响资产情况，相关产品如下：

【深信服云镜 YJ】 已发布资产检测方案，指纹 ID:0032395。

【深信服漏洞评估工具 TSS】已发布资产检测方案，指纹 ID:0032395。

五、时间轴

2026/03/17　深瞳漏洞实验室监测到 OpenClaw WebSocket 共享令牌权限提升漏洞信息。

2026/03/17　深瞳漏洞实验室发布漏洞通告。

六、参考链接

https://github.com/openclaw/openclaw/security/advisories/GHSA-rqpp-rjj8-7wv8

七、了解更多

深信服千里目安全技术中心持续紧跟国内外漏洞威胁情报，从中筛选出能给客户带来威胁的漏洞，第一时间推送解决方案，持续提供可感知的安全感。在这场永不停歇的攻防战争中，深信服千里目安全技术中心掌握一手漏洞情报，坚持“千里之外，洞悉风险”，与各大网络安全厂商一同维护网络安全，构建平衡、和谐的网络生态系统。关注深信服千里目安全技术中心微信公众号，第一时间了解更多漏洞情报。