⚠ RELATÓRIO DE SEGURANÇA

OpenClaw Security Crisis

Vulnerabilidades críticas identificadas em 2025–2026 · Gerado em 15 de março de 2026

10+
CVES PUBLICADOS

8.8
CVSS MÁXIMO

297
ATAQUES/24H (MÉDIA)

100s
SKILLS MALICIOSAS

Vulnerabilidades Críticas

CVE-2026-25253 One-Click RCE via Cross-Site WebSocket Hijacking — CVSS 8.8

Vulnerabilidade crítica de execução remota de código sem autenticação. O Control UI do OpenClaw confiava no parâmetro `gatewayUrl` da query string sem validação, permitindo que um atacante roubasse o token de autenticação com um único clique em um link malicioso. Até instâncias configuradas em `localhost` eram vulneráveis.

Descoberto por: Mav Levin (depthfirst research) Corrigido: v2026.1.29 (30 jan 2026) Divulgado: 3 fev 2026

RCE · Sem Autenticação · WebSocket Hijacking

CVE-2026-24763 Bypass do Sandbox Docker — CVSS 8.x

Bypass do isolamento do sandbox Docker após a correção incompleta do CVE-2026-25253. Permitia que um atacante escapasse do container e executasse código na máquina host.

Corrigido: v2026.1.30

Container Escape RCE

CVE-2026-26319 Autenticação Ausente em Endpoints Críticos

CVSS 7.x

Endpoints da API do gateway sem verificação de autenticação. Pesquisadores da Endor Labs identificaram que diversas rotas internas aceitavam requisições sem token válido, expondo dados sensíveis e operações privilegiadas.

Descoberto por: Endor Labs Fevereiro 2026

Missing Auth API Exposure

CVE-2026-26329 Path Traversal

CVSS 6.x

Vulnerabilidade de path traversal que permitia leitura de arquivos arbitrários no sistema de arquivos do servidor. Um atacante autenticado podia acessar arquivos fora do diretório permitido, incluindo chaves privadas e configurações.

Descoberto por: Endor Labs Fevereiro 2026

Path Traversal Info Disclosure

CVE-2026-26322 / GHSA-56f2 / GHSA-pg2v Server-Side Request Forgery (SSRF)

CVSS 6.x

Múltiplas vulnerabilidades SSRF permitiam que um atacante manipulasse o servidor para fazer requisições HTTP para redes internas, expondo serviços internos e metadados de cloud (AWS IMDSv1, GCP metadata endpoint, etc.).

Descoberto por: Endor Labs Fevereiro 2026

SSRF Internal Network

Linha do Tempo

Novembro 2025

Lançamento do OpenClaw (ex-Clawdbot)

Projeto lançado com crescimento rápido de adoção. A filosofia de "deploy fácil" priorizou conveniência em detrimento da segurança.

Janeiro 2026

CVE-2026-25157 — Primeiro patch de segurança

Primeira vulnerabilidade pública corrigida em v2026.1.25 (25 jan).

Jan–Fev 2026

☠ Campanha ClawHavoc — Supply-Chain Attack

Centenas de skills maliciosas publicadas no ClawHub (marketplace oficial). Disfarçadas com documentação profissional, instalavam malwares como AMOS (Atomic macOS Stealer) e keyloggers que exfiltravam API keys.

30 Jan 2026

CVE-2026-25253 corrigido — v2026.1.29/30

One-click RCE crítico (CVSS 8.8) e bypass de sandbox Docker corrigidos. Patch incompleto na primeira versão, necessitando v2026.1.30.

Fevereiro 2026

Endor Labs publica 6 novas CVEs

SSRF (3 variantes), missing auth, path traversal e outros problemas arquiteturais revelados publicamente.

Março 2026

□□ China emite diretrizes oficiais

MIIT e NVDB da China publicam alertas e boas práticas para usuários OpenClaw, recomendando atualização imediata e minimização de exposição à internet.

⚡Vetores de Ataque Identificados

Prompt Injection via Web

Agentes OpenClaw com acesso à web foram manipulados por páginas contendo instruções maliciosas embutidas. O agente executava comandos não autorizados, vazava chaves de API e realizava ações em nome do usuário sem consentimento.

Supply-Chain via ClawHub (ClawHavoc)

O marketplace oficial ClawHub foi utilizado como vetor de distribuição de malware. Skills com documentação convincente escondiam código que:

- Exfiltrava chaves de API (OpenAI, Anthropic, Google)
- Instalava keyloggers persistentes
- Enviava dados do `openclaw.json` para servidores externos

Instâncias Expostas na Internet

Milhares de instâncias com gateway exposto em `0.0.0.0` sem autenticação foram indexadas e exploradas. Pesquisadores encontraram tokens de autenticação, chaves de API e arquivos de configuração completos publicamente acessíveis.

□Status desta Instância

Esta instância está protegida

- Gateway escutando em `127.0.0.1` (loopback) — não exposto à internet
- Acesso externo via Tailscale (rede privada criptografada)
- dmPolicy configurado como `pairing` — apenas dispositivos autorizados

- UFW ativo — apenas porta SSH (22) aberta
- Fail2ban ativo — IPs com brute force são banidos automaticamente
- API keys movidas para variáveis de ambiente (`.env` com chmod 600)
- Versão atualizada: v2026.3.13

Recomendações Gerais

- Mantenha sempre a versão mais recente do OpenClaw instalada
- Nunca exponha o gateway em `0.0.0.0` — use Tailscale ou Cloudflare Tunnel
- Ative autenticação por token ou pairing obrigatório
- Instale skills apenas de fontes confiáveis e verificadas
- Nunca hardcode API keys no `openclaw.json` — use variáveis de ambiente
- Configure UFW para bloquear todas as portas desnecessárias
- Ative Fail2ban para proteção contra brute force no SSH
- Revise periodicamente os logs de acesso e tentativas bloqueadas

Fontes

The Hacker News — One-Click RCE (CVE-2026-25253)

SonicWall — Auth Token Theft Analysis

Infosecurity Magazine — 6 novas CVEs (Endor Labs)

Conscia — The OpenClaw Security Crisis

Kaspersky — Vulnerabilities Exposed

runZero — Architectural Weaknesses
