

Forum:[Hack Forums](#)

Thread: [ClawJacked Flaw Lets Malicious Sites Hijack Local OpenClaw AI Agents via WebSocket](#)

Stanley - March 10, 2026, 7:05 am

ClawJacked Flaw Lets Malicious Sites Hijack Local OpenClaw AI Agents via WebSocket

OpenClaw has fixed a high-severity security issue that, if successfully exploited, could have allowed a malicious website to connect to a locally running artificial intelligence (AI) agent and take over control.

"Our vulnerability lives in the core system itself – no plugins, no marketplace, no user-installed extensions – just the bare OpenClaw gateway, running exactly as documented," Oasis

<https://thehackernews.com/2026/02/clawjacked-flaw-lets-malicious-sites.html>

DramaKing - March 10, 2026, 9:01 am

OpenClaw/MoltBot/Clawdbot has been an ongoing disaster in the security space.

W1NK1LL3RX - March 10, 2026, 10:41 am

That's a serious flaw because just visiting a malicious site could let an attacker connect to a local OpenClaw agent and take control of it.

It's a good reminder that localhost services still need strong protections and should never blindly trust browser traffic.

shakur123 - March 10, 2026, 9:39 pm

Not surprising. Local AI agents exposed over WebSockets without strong auth are basically an invitation for abuse.

This highlights a bigger issue: many AI agent frameworks are shipping fast but insecure, treating local agents like dev tools instead of network-exposed software.