Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

One Click to Compromise: Inside OpenClaw's Critical RCE Flaw

Date of Publication	Admiralty Code	TA Number
February 03, 2026	A1	TA2026033

Summary

First Seen: January 26, 2026
Affected Products: OpenClaw (aka Clawdbot/Moltbot)
Impact: CVE-2026-25253 is a high-impact remote code execution vulnerability in the open-source AI agent OpenClaw (Clawdbot/Moltbot) caused by improper trust of a user-controlled gatewayUrl parameter. A single malicious link can trigger a "1-click" exploit that leaks authentication tokens and enables WebSocket hijacking, allowing attackers to execute arbitrary commands on the victim's local system. The attack requires no prior authentication and bypasses local network protections by leveraging the victim's browser to access localhost services. Developer environments are particularly at risk due to common use of local and privileged deployments. All versions prior to v2026.1.29 are affected and should be patched immediately, with exposed credentials rotated.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-25253	OpenClaw Remote Code Execution Vulnerability	OpenClaw	✗	✗	✓

Vulnerability Details

#1 CVE-2026-25253 is a high-severity remote code execution vulnerability affecting the open-source AI agent OpenClaw (also known as Clawdbot or Moltbot). The flaw originates from improper trust of a user-supplied gatewayUrl parameter, causing the application to automatically establish a WebSocket connection without sufficient validation.

#2 An attacker can exploit this issue through a single malicious link or webpage, researchers describe it as a "1-Click RCE Kill Chain" that executes in milliseconds. When a victim interacts with the crafted URL, OpenClaw inadvertently transmits its authentication token to an attacker-controlled endpoint. The attacker can then hijack the WebSocket session to gain unauthorized access to the local OpenClaw instance, resulting in arbitrary command execution. This technique effectively bypasses local network protections by abusing the victim's browser as a bridge to localhost services.

#3 The attack requires no prior authentication or special privileges, making it particularly dangerous in developer environments where OpenClaw often runs locally or with elevated permissions. The risk is further amplified by missing WebSocket origin validation, enabling cross-site WebSocket hijacking and full instance compromise.

#4 All OpenClaw versions prior to v2026.1.29 are affected. Proof-of-concept exploits are publicly available, increasing the likelihood of active exploitation. Users should upgrade immediately, rotate any exposed tokens or credentials, and review logs for suspicious WebSocket activity. Due to its low interaction cost and high impact, this vulnerability should be treated as critical in any environment using OpenClaw.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2026-25253	OpenClaw Clawdbot/Moltbot (Before 2026.1.29)	cpe:2.3:a:openclaw:openclaw:*:*:*:*:*:*:*:*	CWE-669

Recommendations

Update OpenClaw Immediately: Install the latest version of OpenClaw (2026.1.29 or later) without delay. This patch addresses the vulnerability by implementing a gateway URL confirmation modal that requires explicit user approval before connecting to new gateway URLs, eliminating the automatic token exfiltration attack vector. Organizations should prioritize this update as the vulnerability is trivially exploitable and proof-of-concept code is publicly available.

Rotate All Authentication Credentials: After applying the patch, immediately generate a new authToken for all OpenClaw instances. Additionally, rotate API keys for all connected services including messaging platforms (Slack, Discord, Telegram), cloud providers (AWS, GCP, Azure), and any other integrated services. Assume that credentials may have been compromised if your instance was running an unpatched version, particularly if users may have visited untrusted websites while the OpenClaw interface was active.

Audit System Logs for Suspicious Activity: Review authentication logs, WebSocket connection logs, and command execution histories for any anomalies dating back to January 26, 2026 or earlier. Search specifically for unexpected WebSocket connections to external IP addresses, unauthorized configuration changes to sandbox settings or approval policies, and execution logs containing suspicious commands such as process.mainModule.require, child_process, or execSync patterns.

Implement Network Segmentation: Restrict the OpenClaw Control UI to trusted network segments only and avoid exposing the interface to the public internet. Consider implementing VPN requirements for administrative access and deploy web application firewalls to detect and block malicious URL parameters targeting the gatewayUrl vulnerability.

Deploy Browser Security Controls: Implement Content Security Policy headers and consider deploying browser isolation technologies for users who access OpenClaw interfaces. Train users to recognize social engineering attacks that may attempt to redirect them to malicious URLs designed to exploit this vulnerability.

Vulnerability Management: Maintain an inventory of all OpenClaw deployments across your organization and implement automated vulnerability scanning to detect unpatched instances. Establish a process for monitoring security advisories from the OpenClaw project and evaluate implementing a containerized deployment strategy with restricted network access to minimize the impact of future vulnerabilities.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1566: Phishing	T1566.002: Spearphishing Link
Credential Access	T1528: Steal Application Access Token	
Execution	T1204: User Execution	T1204.001: Malicious Link
	T1059: Command and Line Interface	
Command and Control	T1071: Application Layer Protocol	T1071.001: Web Protocols
	T1102: Web Service	
Privilege Escalation	T1068: Exploitation for Privilege Escalation	

Patch Details

Upgrade OpenClaw to version 2026.1.29 or later.

Link:
https://github.com/openclaw/openclaw/releases

References

https://ethiack.com/news/blog/one-click-rce-moltbot

https://depthfirst.com/post/1-click-rce-to-steal-your-moltbot-data-and-keys

https://openclaw.ai/blog/introducing-openclaw

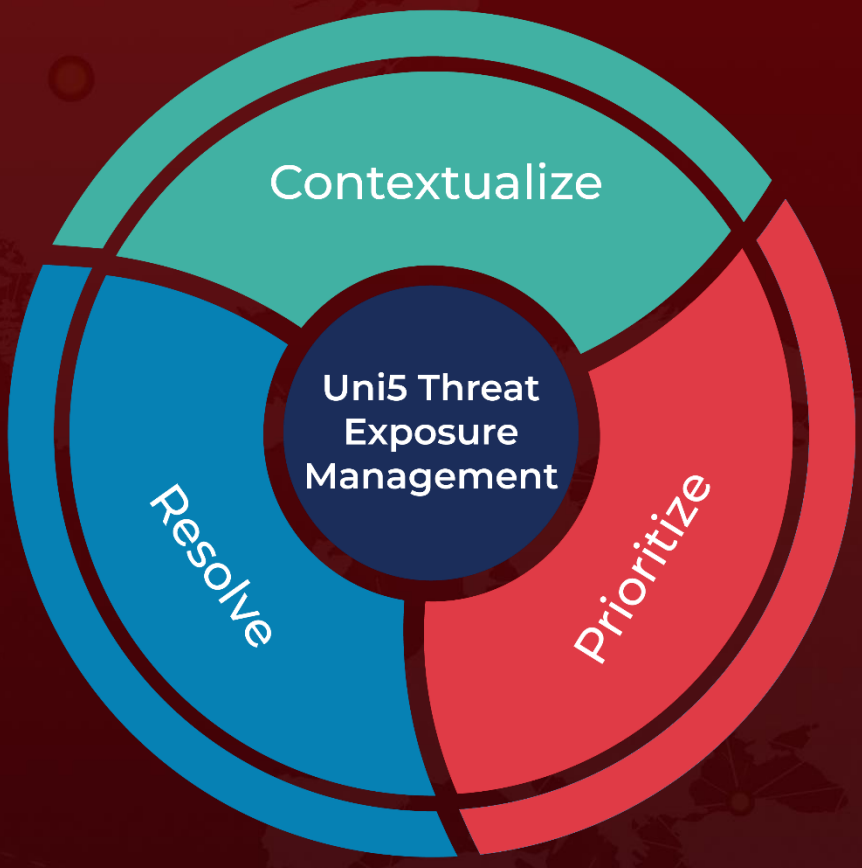
https://github.com/openclaw/openclaw/security/advisories/GHSA-g8p2-7wf7-98mq

https://github.com/ethiack/moltbot-1click-rce

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

February 03, 2026 • 07:30 AM

More at www.hivepro.com