interweb

Generated on 15/11/2026 01:42

KNOWLEDGE BASE · PUBLIC DOCUMENT

OpenClaw security: what it can reach, and how to limit it

Agents & AI on a VPS

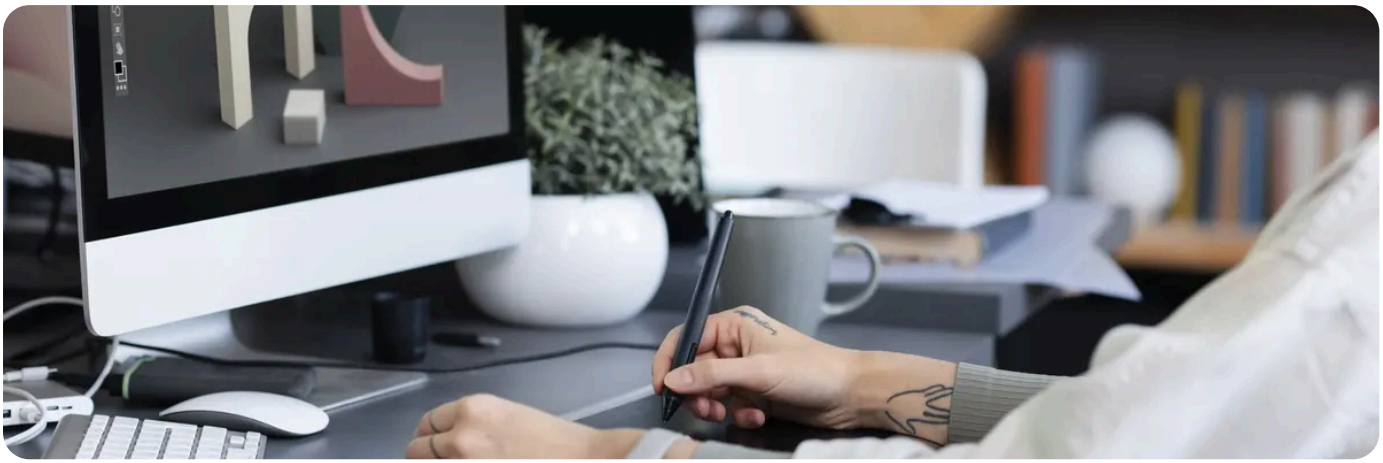
CODE	VERSION	COUNTRY · LANGUAGE
RLX-MZ-KB-944	v2026.10.10	Mozambique · English

Interweb Mozambique
RLX Holdings, S.A. · Group RLX Holdings
Tax ID (NUIT) 401 191 607 · Legal entity no. (NUEL) 105 045 974 · Economic activity code (CAE) 62022

https://www.meu.interweb.co.mz/knowledgebase/944

OpenClaw security: what it can reach, and how to limit it

Agents & AI on a VPS Created on **October 10, 2026** 3 min read



OpenClaw has access to files, commands and accounts, and it acts on your behalf. So the right security question is not "is the program safe?", it is **"what happens on the worst day, and how much damage can it do?"**. You control the answer with four decisions: a user of its own, with no permanent root; minimum permissions; a server that holds nothing else important; and spending limits at the model provider.

This holds for any agent that executes things, not just this one. There is no way to guarantee that an AI model is always right, or that it ignores bad instructions hidden in a text. That is why you limit its reach instead of trusting it.

What it can reach

Reach	The risk	The limit to set
Files on the server	Reading secrets, deleting or changing data	Run it as a user with no access to your other applications and files
Commands	Running something destructive, by mistake or by malicious instruction	No permanent root. No free `sudo` for that user.
Accounts and keys	Spending money or sending on your behalf	Keys with only the permissions needed, and a spending limit at the provider
Messaging channels	Anyone who writes to it can give it orders	Authorised accounts only. See **connecting a channel**.
Network	Ports open to the internet	Only the ones you need, with the firewall on

How to limit it, in order

1. **A server just for it.** Do not install it on the VPS that holds the website, the shop or the company database. A test server, easy to rebuild, is the right place to start.

2 **A user of its own, no permanent root.** Log in as root only to prepare things. After that, OpenClaw runs as a normal user that only sees its own folder.

3 **Minimum permissions.** Give it only the folders and accounts the task needs. If the documentation offers a mode that asks for confirmation before sensitive actions, use it, and remember that a confirmation only protects you if you read it.

4 **Keys with limits.** Create an API key just for this agent and, in the provider's console, set a spending limit if the provider allows it. See **getting a key and keeping it safe**.

5 **Close the rest.** Keep the firewall on and SSH protected, as in **keeping your VPS secure**.

6 **Have a way back.** A snapshot before you give it new powers. See **backing up a VPS**.

! **Hidden instructions.**
If the agent reads a web page, an e-mail or a file containing text like "ignore what you were asked and do this", it may obey. The more unknown sources it reads, the greater the risk. Do not give it access to sensitive things and to strangers' content at the same time.

! **Never give the agent**
your control-panel password, your domain keys, your mailbox key or customer data just because it is "easier". Whatever it reads may pass through the model provider.

Read the logs now and then. If commands show up that you did not ask for, switch the agent off, revoke the keys and restore the snapshot. See **running OpenClaw day to day**.

NEED A HAND?

Want to be sure your VPS is closed the way it should be? Ask us for help with the server's access and network.

Open a support ticket →

SEE ALSO

What OpenClaw is, and what you need to run it →

- **Keeping your VPS or dedicated server secure: the six that matter** →
- **AI hallucinations: how to check an answer before you use it** →
- **Support Policy** →

interweb

Interweb Mozambique

RLX Holdings, S.A. · Group RLX Holdings

TAX ID (NUIT)	401 191 607
LEGAL ENTITY NO. (NUEL)	105 045 974
ECONOMIC ACTIVITY CODE (CAE)	62022
REGISTERED OFFICE	Bairro 7 de Setembro Vilankulo 1304 · CEP 0411-02, Inhambane, Mozambique
CONTACT	info@interweb.co.mz · +258 84 635 1111 · +258 86 635 1111 · www.interweb.co.mz
OPENING HOURS	Monday to Friday - 08 AM to 04 PM Saturday & Sunday - Closed

Online version of this document

RLX-MZ-KB-944 · v2026.10.10 · Generated on 15/11/2026 01:42