Generated on 21/10/2026 17:45

KNOWLEDGE BASE · PUBLIC DOCUMENT

Is my VPS compromised? Checking processes, cron jobs, users, SSH keys and temporary folders

Security

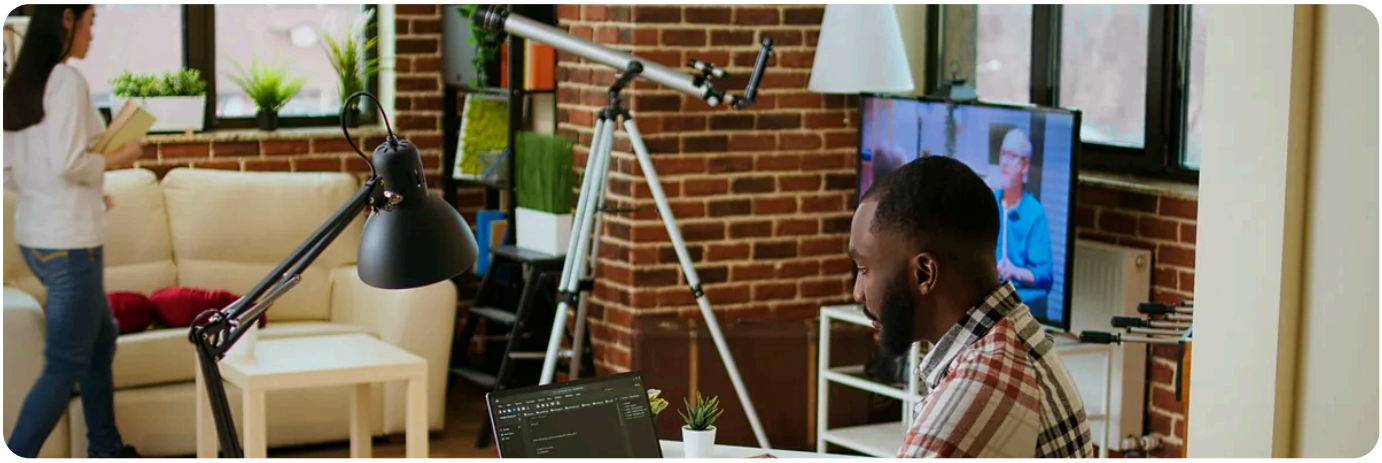
CODE	VERSION	COUNTRY · LANGUAGE
RLX-MZ-KB-2247	v2026.10.21	Mozambique · English

MozOut 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.mozout.co.mz/knowledgebase/2247

Is my VPS compromised? Checking processes, cron jobs, users, SSH keys and temporary folders

Security Created on **October 21, 2026** 4 min read



The short answer: this article is for **VPS and dedicated server** customers with root access. After an abuse notice, or when the server behaves oddly (CPU always high, connections you do not recognise), there are **eight places to look**: processes, network connections, cron jobs, services, users, login records, SSH keys and temporary folders. The commands below **only read**: they change nothing. Before deleting anything you find, **take a copy for analysis**.

Where to look, and what is suspicious

What to check	Command	What is suspicious
Processes	`ps auxf`, `top` or `htop`	Random names, names that imitate system processes, programs running from `/tmp` or `/dev/shm`, CPU always at the top.
Network connections	`ss -tunap` or `lsof -i`	Many outgoing connections to addresses you do not know, or a program listening on a port you did not open.
Cron jobs	`crontab -l` for each user, `/etc/cron*`	Lines that download and run something (`curl` or `wget` with `| sh`), base64 text.
Services and timers	`systemctl list-units --type=service`, `systemctl list-timers`	Services with names you do not recognise, or that start a file from a temporary folder.
Users	`/etc/passwd`	New users with a shell, or a user other than root with UID 0.
Logins	`last` and `lastb`	Logins from IPs that are not yours; many failed attempts (password guessing).

What to check	Command	What is suspicious
SSH keys	`~/.ssh/authorized_keys` for root and each user	Keys you do not recognise: they let someone in without a password.
Temporary folders	`/tmp`, `/var/tmp`, `/dev/shm`	Executable files, hidden files (starting with a dot), folders with odd names.

The check, step by step

1. **Log in over SSH as root, or as a user with sudo,** and note the time you start. If you lost access, see **I have lost SSH access** and tell us in the support ticket.

2. **Run the read-only commands in the block below,** one at a time, and keep what they show (in a file or a note). Compare it with what you know you installed.

3. **For each suspicious item, find where it comes from:** the program behind a process shows with `ls -l /proc/PID/exe` (replace PID with the process number). The logs help to date the break-in: **where the logs are on a VPS**.

4. **Before deleting, copy for analysis** (second block below). The copy and its SHA-256 sum are useful for the report and for understanding what happened.

5. **Decide: reinstall or clean in place.** If you found a user other than root with UID 0, keys that are not yours or programs hidden in the system, reinstall. If you are cleaning, remove the cron entries, services, keys and odd users first, and only then stop the processes.

6. **Close the way in:** change every password, switch to **SSH keys**, update the system and the applications, and close in the firewall whatever does not need to be open. Then write the report: **writing the reply to an abuse notice**.

The read-only commands

Run them as root (or with `sudo` in front). None of them changes anything on the server: `ps auxf`

```
ss -tunap
for u in $(cut -d: -f1 /etc/passwd); do crontab -l -u "$u" 2>/dev/null | sed "s/^/$u:/"; done
ls -la /etc/cron* /var/spool/cron 2>/dev/null
systemctl list-units --type=service --state=running
systemctl list-timers
awk -F: '$3 == 0' /etc/passwd
```

```
last -a | head -30
lastb -a | head -30
cat /root/.ssh/authorized_keys
ls -la /tmp /var/tmp /dev/shm
```

Copy before you delete

Keep a copy of each suspicious file in a folder of your own, with its SHA-256 sum, before deleting it. Do not leave it in a public folder of the site:

```
mkdir -p /root/analise
cp -a /caminho/do/ficheiro-suspeito /root/analise/
sha256sum /root/analise/*
```

An attacker with root can hide from the very commands you use.
If the system was altered, `ps` and `ss` can lie, and a server that "looks clean" may not be. **On a compromised server, the safest route is to reinstall the system and restore a clean copy** (**reinstalling the VPS operating system** and **which backup to restore**). Cleaning in place is for people who know what they are doing: an attacker with root access can leave ways back in that are not obvious at first. Never run the suspicious files to "see what they do".

Lots of lines in `lastb` do not mean someone got in:
They are failed attempts, common on any server with SSH open. They are cut down with **fail2ban** and key-only login. What matters is `last`: the logins that succeeded.

NEED A HAND?

Found something and cannot tell whether it is yours or an attacker's? Send us the command output in the support ticket.

Open a support ticket →

SEE ALSO

- Your VPS is scanning other networks: finding and stopping the process behind a netscan notice →
- Writing the reply to an abuse notice: cause, what you removed and how it will not happen again →
- Where are the logs on a Linux VPS: journalctl and /var/log →
- How to create an SSH key and log in to your VPS without a password →

- Reinstalling or changing your VPS operating system
- After a hack, which backup do you restore? Choosing a clean copy

MozOut 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@mozout.co.mz · +258 84 635 1111 · +258 86 635 1111 · www.mozout.co.mz
OPENING HOURS	Monday to Friday - 08 AM to 04 PM Saturday & Sunday - Closed

Online version of this document

RLX-MZ-KB-2247 · v2026.10.21 · Generated on 21/10/2026 17:45