Generated on 21/10/2026 20:42

KNOWLEDGE BASE · PUBLIC DOCUMENT

An open DNS resolver on your VPS: why it is used in attacks and how to turn off recursion

Security

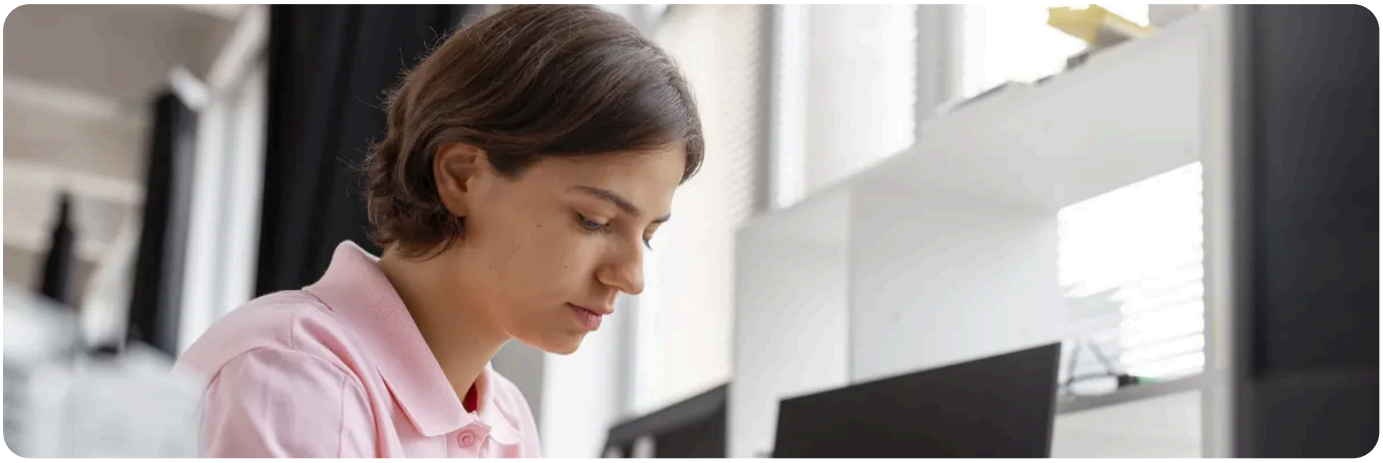
CODE	VERSION	COUNTRY · LANGUAGE
RLX-MZ-KB-2253	v2026.10.21	Mozambique · English

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/2253

An open DNS resolver on your VPS: why it is used in attacks and how to turn off recursion

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



For VPS and dedicated server customers with root access. The short answer: an open DNS resolver answers questions about **any** domain from **any** address on the internet, on port **53**. Attackers send it small queries with a forged source address (the victim's), and your server sends the victim much larger answers: an amplification attack, and your VPS takes part without ever being hacked. A national incident response team (CERT) finds these resolvers and our network and data centre provider sends us the notice. The fix is to turn off **recursion** for outsiders, or the whole service if you do not need it, without breaking DNS for any domains the server hosts.

What may be answering on port 53

What runs	What to do
BIND (`named`), installed by a panel or by hand as the name server for your domains	Keep it answering for your domains, with recursion off (or allowed only for the server itself).
BIND or Unbound installed just so the server can resolve names	Make it listen on 127.0.0.1 only and refuse everyone else.
dnsmasq, Pi-hole or AdGuard Home in a container with port 53 published	Stop publishing it to the outside, or limit it in the firewall to the addresses that use it (your VPN, for example).
systemd-resolved on `127.0.0.53`	Not an open resolver: it only listens locally. Leave it alone.
A process you do not recognise	Treat it as suspicious: **is my VPS compromised?**.

Closing the resolver

1. **See what listens on port 53:** `sudo ss -tulnp | grep ":53 "` Addresses `0.0.0.0`, `[::]` or the public IP mean it answers the outside world.

2. **Test from another machine:** `dig @YOUR_SERVER_IP example.com`. An address in the ANSWER section and the `ra` flag mean the resolver is open. `status: REFUSED` or a timeout means it is closed. Reading the output: **dig and nslookup**.

3. **Ask whether this server needs DNS at all.** Check where your domains point with `dig NS asuaempresa.co.mz`. If they use the registrar's name servers or another service, not this VPS, you can switch the service off: `sudo systemctl disable --now named` (or `bind9`, `unbound`, `dnsmasq`, whichever is running).

4. **BIND serving your domains:** inside the existing `options` block (`/etc/bind/named.conf.options` on Debian and Ubuntu; `/etc/named.conf` on the Red Hat family), add: `recursion no;`
`allow-query-cache { none; };` If the server itself uses BIND to resolve names, use this instead: `allow-recursion { 127.0.0.1; ::1; };`
`allow-query-cache { 127.0.0.1; ::1; };` Check and restart: `sudo named-checkconf`
`sudo systemctl restart named` (on older Debian and Ubuntu releases the service is `bind9`).

5. **Unbound:** in the `server:` section of `unbound.conf`: `interface: 127.0.0.1`
`access-control: 0.0.0.0/0 refuse`
`access-control: 127.0.0.1/8 allow` Then `sudo unbound-checkconf`
`sudo systemctl restart unbound`

6. **dnsmasq or a container:** for dnsmasq, `listen-address=127.0.0.1` and `bind-interfaces`. For a container, change `"53:53/udp"` to `"127.0.0.1:53:53/udp"` (and the same for tcp), or drop the mapping, then `docker compose up -d`. Remember that ufw does not stop ports published by Docker: **Docker on a VPS, safely**.

7. **Repeat the step 2 test** from outside and keep the output for your report.

8. **Reply to the support ticket** in My MozOut, within the notice's deadline (short, often a single day), with a short report: the cause, what you changed and how you checked that the port no longer answers from outside. There is a template in **writing the reply to an abuse notice**. With no reply, or if the problem carries on, the server may be switched off to protect the network, with your data left intact: **why a server is switched off and how to bring it back**.

! **Do not close port 53 or stop BIND on a server that is the name server for your domains:** The websites and e-mail of those domains can no longer be found. On a name server, 53 stays open (UDP and TCP) and what you close is recursion. Copy the configuration files before editing them.

This notice does not mean the server was hacked:

An open resolver is abused from outside, just as it is. A reply to the notice is still required, and the attack traffic stops once recursion is closed. On a VPS, root access is yours: we do not log in to the server and cannot change a firewall that runs inside it. If you lose SSH, tell us in the support ticket.

NEED A HAND?

Not sure whether your VPS is the name server for your domains? Tell us the domains and the step 1 output in the support ticket.

Open a support ticket →

SEE ALSO

- An abuse notice about your server: what it means, the deadline and what we need from you
- Writing the reply to an abuse notice: cause, what you removed and how it will not happen again
- Checking DNS from the command line: dig and nslookup, and how to read the answer
- Setting up the ufw firewall on Ubuntu without locking yourself out
- Running Docker on a VPS safely: the precautions that matter
- A DDoS attack coming from your server: finding the outgoing flood and stopping it

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-2253 · v2026.10.21 · Generated on 21/10/2026 20:42