Generated on 21/10/2026 20:42

KNOWLEDGE BASE · PUBLIC DOCUMENT

CLDAP, Portmapper and other open UDP services: reflection attacks and how to close them

Security

CODE	VERSION	COUNTRY · LANGUAGE
RLX-MZ-KB-2255	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/2255

CLDAP, Portmapper and other open UDP services: reflection attacks and how to close them

Security Created on **October 21, 2026** 5 min read

For VPS and dedicated server customers with root access. The short answer: some services that speak **UDP** answer a small request with a much bigger reply. UDP does not check who is asking, so attackers forge the source address (the victim's) and use your server to flood the victim's connection: a **reflection** attack. The ones a national incident response team (CERT) reports most are **CLDAP** (from Windows servers running Active Directory) and **Portmapper** (rpcbind, which comes with NFS). You close them like this: switch off what you do not use, make what you do use listen internally only, and let only the addresses that need it through the firewall.

The services these reports name

Service	Port	What to do
CLDAP (Active Directory)	UDP 389	A domain controller should not answer the internet. Limit the inbound rules to your own network or VPN.
Portmapper (rpcbind)	TCP and UDP 111	If you do not use NFS, switch it off. If you do, allow only the servers that mount the shares.
Memcached	UDP and TCP 11211	Listen on 127.0.0.1 only and turn UDP off.
NTP (ntpd serving time)	UDP 123	The server can set its own clock without serving time to others: block inbound. chrony, by default, serves time to nobody.
SNMP	UDP 161	Switch it off unless you monitor the server over SNMP. If you do, allow only the monitoring system's IP.
SSDP, WS-Discovery, NetBIOS	UDP 1900, 3702, 137	Local network services: there is no reason for them to answer the internet. Switch off or block.
DNS resolver	UDP 53	Has its own article: **an open DNS resolver**.

Finding and closing them

1. **List what listens on UDP:** `sudo ss -ulnp` `rpcinfo -p` Anything on `0.0.0.0` or `[::]` listens on every address; `127.0.0.1` only internally. On a Windows VPS, in an administrator command prompt: `netstat -ano -p udp`.

2. **Before switching anything off, check who uses it:** `cat /etc/exports` `findmnt -t nfs,nfs4` The first shows what this server shares over NFS; the second, the NFS shares it mounts. If both are empty and you know of no other use, rpcbind is not needed.

3. **Portmapper, if you do not use NFS:** `sudo systemctl disable --now rpcbind.service rpcbind.socket` `sudo systemctl mask rpcbind.service rpcbind.socket` The `.socket` unit restarts the service on the first request, so both go. `mask` stops another package from turning it back on; undo it with `sudo systemctl unmask rpcbind.service rpcbind.socket`.

4. **CLDAP on a Windows VPS:** if the server does not need to be a domain controller, do not make it one. If it does, open Windows Defender Firewall with Advanced Security, find the Active Directory LDAP inbound rules and, on the scope tab, limit the remote address to your private network or VPN. Names vary with the Windows version and language. See also **making Remote Desktop safer**.

5. **Memcached:** on Debian and Ubuntu, in `/etc/memcached.conf` (on the Red Hat family, in the OPTIONS line of `/etc/sysconfig/memcached`): `-l 127.0.0.1` `-U 0` then `sudo systemctl restart memcached`.

6. **A firewall that refuses all inbound traffic** and opens only what serves the public. Let SSH through **before** changing the default rule: `sudo ufw allow OpenSSH` `sudo ufw default deny incoming` `sudo ufw status verbose` If you moved SSH to another port, allow that port instead of OpenSSH. Without ufw, see the rules with `sudo nft list ruleset`. Guide: **setting up ufw without locking yourself out**.

7. **Test from another machine:** `sudo nmap -sU -p 111,389,11211 YOUR_SERVER_IP` (nmap may not be installed). In a UDP scan, “open|filtered” is normal for a port the firewall blocks; “open” means the service still answers.

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**.

Switching services off blindly can break things:

Rpcbind is needed to mount NFS shares, and Active Directory by the machines that depend on it. Check first (step 2) and, on a domain controller, limit rather than switch off. A wrong firewall rule can lock you out: 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.

These notices do not mean the server was hacked:

The service is abused from outside, just as it is. The rule that prevents the next notice is simple: refuse everything inbound and open only what must be open. See **the six that matter**.

NEED A HAND?

Not sure which program opened one of these ports? Send us 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
- An open DNS resolver on your VPS: why it is used in attacks and how to turn off recursion
- Setting up the ufw firewall on Ubuntu without locking yourself out
- Keeping your VPS or dedicated server secure: the six that matter
- Making Remote Desktop on a Windows VPS safer

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-2255 · v2026.10.21 · Generated on 21/10/2026 20:42