interweb

Gerado a 21/10/2026 11:47

BASE DE CONHECIMENTO · DOCUMENTO PÚBLICO

CLDAP, Portmapper e serviços UDP abertos à internet: ataques de reflexão e como fechá-los

Segurança

CÓDIGO	VERSÃO	PAÍS · IDIOMA
RLX-AO-KB-2256	v2026.10.21	Angola · Português

Interweb Angola
RLX Angola, Lda. · Grupo RLX Holdings
NIF 500 260 5724 · Matrícula 26464-25/250724

https://www.meu.interweb.ao/knowledgebase/2256

Para quem tem um VPS ou um servidor dedicado com acesso root. A resposta curta: alguns serviços que falam por **UDP** respondem a um pedido pequeno com uma resposta muito maior. Como o UDP não confirma quem pergunta, os atacantes falsificam o endereço de origem (o da vítima) e usam o seu servidor para lhe encher a ligação: é um ataque de **reflexão**. Os mais reportados por uma equipa nacional de resposta a incidentes (CERT) são o **CLDAP** (dos servidores Windows com Active Directory) e o **Portmapper** (rpcbind, que vem com o NFS). Fecham-se assim: desligar o que não usa, pôr a ouvir só por dentro o que usa, e deixar na firewall só os endereços que precisam.

Os serviços que aparecem nestes relatórios

Serviço	Porta	O que fazer
CLDAP (Active Directory)	UDP 389	Um controlador de domínio não deve responder à internet. Limite as regras de entrada aos endereços da sua rede ou VPN.
Portmapper (rpcbind)	TCP e UDP 111	Se não usa NFS, desligue. Se usa, só para os IPs dos servidores que montam as partilhas.
Memcached	UDP e TCP 11211	Ouvir só em 127.0.0.1 e desligar o UDP.
NTP (ntpd a servir a hora)	UDP 123	O servidor pode acertar a sua hora sem a servir a outros: bloqueie a entrada. O chrony, por omissão, não serve a hora a ninguém.
SNMP	UDP 161	Desligue se não monitoriza o servidor por SNMP. Se monitoriza, só para o IP do sistema de monitorização.
SSDP, WS-Discovery, NetBIOS	UDP 1900, 3702, 137	São serviços de rede local: não têm razão para responder à internet. Desligue ou bloqueie.
Resolver DNS	UDP 53	Tem artigo próprio: **um resolver DNS aberto**.

Como os encontrar e fechar

1 **Liste o que ouve em UDP:** `sudo ss -ulnp` `rpcinfo -p` O que mostra `0.0.0.0` ou `[::]` ouve em todos os endereços; `127.0.0.1` só por dentro. Num VPS Windows, numa linha de comandos de administrador: `netstat -ano -p udp`.

2 **Antes de desligar, confirme quem usa:** `cat /etc/exports` `findmnt -t nfs,nfs4` O primeiro mostra o que este servidor partilha por NFS; o segundo, as partilhas NFS que ele monta. Se os dois vêm vazios e não sabe de mais nenhum uso, o rpcbind não faz falta.

3 **Portmapper, se não usa NFS:** `sudo systemctl disable --now rpcbind.service rpcbind.socket` `sudo systemctl mask rpcbind.service rpcbind.socket` O `.socket` volta a arrancar o serviço ao primeiro pedido, por isso desligam-se os dois. O `mask` impede que outro pacote o volte a ligar; desfaz-se com `sudo systemctl unmask rpcbind.service rpcbind.socket`.

4 **CLDAP num VPS Windows:** se o servidor não precisa de ser controlador de domínio, não o seja. Se precisa, abra a Firewall do Windows Defender com Segurança Avançada, procure as regras de entrada de LDAP do Active Directory e, no separador do âmbito, limite o endereço remoto à sua rede privada ou VPN. Os nomes variam com a versão e a língua do Windows. Veja também **tornar o Ambiente de Trabalho Remoto mais seguro**.

5 **Memcached:** em Debian e Ubuntu, no `/etc/memcached.conf` (na família Red Hat, na linha OPTIONS de `/etc/sysconfig/memcached`): `-l 127.0.0.1`
`-U 0` e depois `sudo systemctl restart memcached`.

6 **Firewall a recusar tudo à entrada** e a abrir só o que serve o público. Deixe o SSH passar **antes** de mudar a regra por omissão: `sudo ufw allow OpenSSH`
`sudo ufw default deny incoming`
`sudo ufw status verbose` Se mudou a porta do SSH, autorize essa porta em vez de OpenSSH. Sem ufw, veja as regras com `sudo nft list ruleset`. Guia: **configurar a ufw sem ficar de fora**.

7 **Teste a partir de outra máquina:** `sudo nmap -sU -p 111,389,11211 IP_DO_SERVIDOR` (o nmap pode não estar instalado). Num teste UDP, «open|filtered» é o normal para uma porta fechada pela firewall; «open» quer dizer que o serviço ainda responde.

8 **Responda ao pedido de suporte** no Meu Interweb, dentro do prazo do aviso (curto, muitas vezes de um dia), com um relatório curto: a causa, o que mudou e como confirmou que a porta já não responde de fora. Há um modelo em **responder a um aviso de abuso**. Sem resposta, ou se o problema continuar, o servidor pode ser desligado para proteger a rede, com os dados intactos: **porque o servidor é desligado e como o voltar a ligar**.

Desligar serviços às cegas pode partir coisas: o rpcbind é preciso para montar partilhas NFS, e o Active Directory para os postos que dependem dele. Confirme primeiro (passo 2) e, num controlador de domínio, limite em vez de desligar. Uma regra de firewall errada pode deixá-lo fora do servidor: Num VPS o acesso root é seu: nós não entramos no servidor nem mudamos a firewall que está lá dentro. Se ficar sem SSH, diga-nos no pedido de suporte.

Estes avisos não querem dizer que o servidor foi invadido: o serviço é usado de fora, tal como está. A regra que evita o próximo aviso é simples: recusar tudo à entrada e abrir só o que precisa de estar aberto. Ver **as seis que contam**.

Não sabe que programa abriu uma destas portas? Envie-nos no pedido de suporte o resultado do passo 1.

Abrir pedido de suporte

VEJA TAMBÉM

Um aviso de abuso sobre o seu servidor: o que significa, o prazo e o que precisamos de si

Responder a um aviso de abuso: a causa, o que removeu e como não se vai repetir

Um resolver DNS aberto no seu VPS: porque é usado em ataques e como desligar a recursão

Configurar a firewall ufw no Ubuntu sem ficar de fora do servidor

Manter o seu VPS ou servidor dedicado seguro: as seis que contam

Tornar o Ambiente de Trabalho Remoto de um VPS Windows mais seguro

interweb

Versão online deste documento

A Interweb é uma empresa líder em serviços de internet, com a missão de ajudar negócios a nascerem e prosperarem por meio da tecnologia.

2020
FUNDADA

37 mil+
CLIENTES

130+
INSCRIÇÕES POR DIA

Interweb Angola

RLX Angola, Lda. · Grupo RLX Holdings

NIF	500 260 5724
MATRÍCULA	26464-25/250724
SEDE	Rua Direita do Patriota, Bairro Dangereux Belas, Luanda, Angola
CONTACTOS	info@interweb.ao · +244 942 011 191 · www.interweb.ao
HORÁRIO	2ª. à 6ª. Feira - 08 à 16 Horas Sábado & Domingo - Fechado

RLX-AO-KB-2256 · v2026.10.21 · Gerado a 21/10/2026 11:47