

KNOWLEDGE BASE · PUBLIC DOCUMENT

An abuse notice about your server: what it means, the deadline and what we need from you

Security

CODE

RLX-MZ-KB-2242

VERSION

v2026.10.21

COUNTRY · LANGUAGE

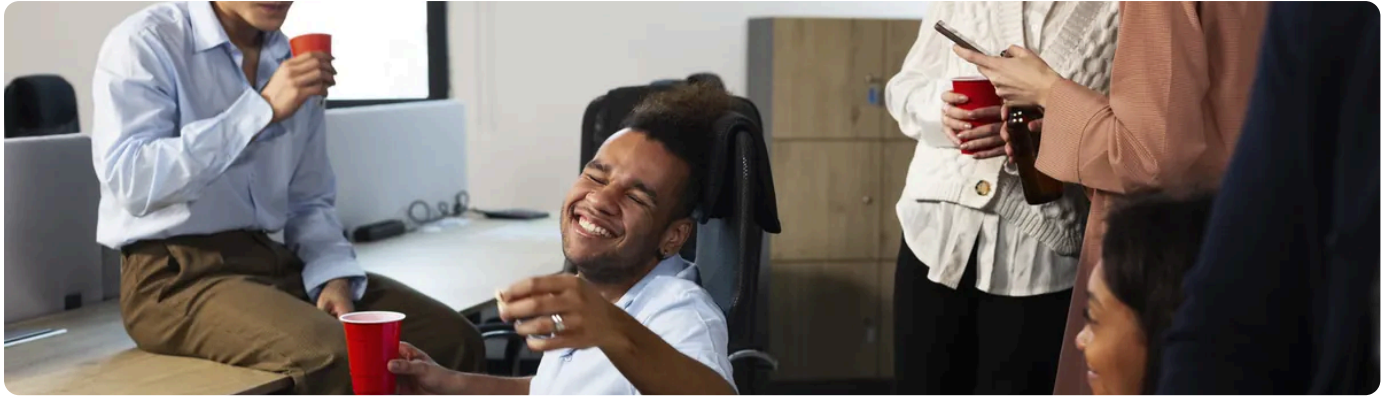
Mozambique · English

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/2242>



The short answer: our network provider watches the traffic. When it sees an attack coming from one of our servers, receives a complaint from someone else, or gets a report from a national incident response team (CERT), it sends us an **abuse notice** with an identifier, a log of what it saw and a **short deadline, often one day**, to fix it and reply. We forward it to you as a **support ticket** in Meu Interweb and ask you for a **short report**: the cause, what you removed and what you did so it does not happen again. This article is for **VPS and dedicated server** customers; the notices about websites (phishing, fraud) also apply to hosting plans.

Which notice you got, and where to read about it

The notice is about	What it means	Where to read
Netscan (network scanning)	Your server opened many connections to a range of addresses, on the same ports, within minutes.	Your VPS is scanning other networks
DDoS from the server	A flood of traffic is leaving your server towards a target.	A DDoS attack coming from your server
Open Redis	Redis answers anyone on the internet and can be used in attacks.	Redis open to the internet
Open DNS resolver	The server answers DNS questions from anyone and helps amplify attacks.	An open DNS resolver
CLDAP, Portmapper (rpcbind) or another UDP service	An open UDP service used for reflection attacks.	UDP services open to the internet
MySQL, MariaDB or PostgreSQL reachable from outside	The database accepts connections from any address.	Databases reachable from the internet
Vulnerable n8n or a web application with critical flaws	A version with known flaws is exposed.	A vulnerable n8n or web application
Phishing	Pages imitating banks or delivery companies on your site, or phishing e-mails leaving the server.	Phishing pages on your site or server
Spam blacklist (Spamhaus, SpamCop)	The server IP was listed for sending spam.	Your server IP is on a spam blacklist
Botnet or command and control (C2)	The server is part of a network of machines controlled by someone else.	Botnet activity from your server
Fraudulent site	A complaint that a site on your account deceives people (fake investment, fake shop).	A fraud complaint about a site
You do not know where to start	The notice does not say the cause, only what was seen from outside.	Is my VPS compromised?

What happens, from notice to reply

1

The network provider sends us the notice, with an identifier, the date and time **in UTC**, the source IP (your server), the destinations and the ports.

2

We forward it to you as a support ticket in Meu Interweb, with the log as it came. Make sure the e-mail on your account is right and that you read new ticket notifications.

3

You investigate your server. On a VPS or dedicated server the root access is yours: we do not log in to the server, and a firewall set up inside it can only be changed by you. Start with **checking whether the VPS is compromised**.

4

You send us the short report, in the same ticket: the cause and how it got in, what you found and removed, and what you did so it does not happen again. The template is in **writing the reply to an abuse notice**.

5

We reply to the provider within the deadline, with your report.

6

First you investigate, with the server still on. If by the deadline the cause is not clear, or the traffic carries on, the server may be switched off to protect the network. The data stays intact. The way back is in **why the server was switched off or locked**.

The times in the notice are in UTC

The log uses UTC; your server logs may be in another time zone. Before searching the log files, check the server time zone and the UTC time side by side: `timedatectl`

`date -u` If the clock is wrong, fix it first: **setting the time zone and the clock on a VPS**.

Do not ignore the notice, or reply only “it is fixed”. Without the cause and what you did, we have nothing to send the provider, and the deadline passes anyway. Deleting the attack file without closing the way in is not enough either: the abuse comes back and the server is switched off again.

Reply early, even before you have everything. One line in the ticket saying what you have done and what is left helps us answer the provider in time. If you lost SSH access, say so in the ticket (**I have lost SSH access**).

Got an abuse notice and cannot make sense of the log? Reply in the ticket itself and we will go through it with you line by line.

[Open a support ticket](#)

SEE ALSO

Writing the reply to an abuse notice: cause, what you removed and how it will not happen again

Why your server was switched off or locked after an abuse notice, and how to bring it back

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

What we do about security, DDoS included, and what stays yours

Keeping your VPS or dedicated server secure: the six that matter

Reporting abuse: how to do it and what happens next



Online version of this document

Interweb is a leading internet services company, with a mission to help businesses to be born and prosper through technology.

2020

FOUNDED

37,000+

CLIENTS

130+

SIGN-UPS A DAY

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