

KNOWLEDGE BASE · PUBLIC DOCUMENT

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

Security

CODE

RLX-AO-KB-2244

VERSION

v2026.10.21

COUNTRY · LANGUAGE

Angola · English

Interweb Angola

RLX Angola, Lda. · Group RLX Holdings

Tax ID (NIF) 500 260 5724 · Commercial registration no. 26464-25/250724

<https://www.meu.interweb.ao/knowledgebase/2244>

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

 Security

 Created on **October 21, 2026**

 4 min read



The short answer: the report we ask for after an abuse notice has **three parts: the cause and how it got in, what you found and removed, and what you did so it does not happen again.** It is what we use to answer our network provider within the deadline. It does not need to be long: it needs to be specific. This article has a template you can copy.

What to write in each part

Part	What works	What does not
Notice identifier	The identifier and the IP, as they appear in the support ticket.	Replying in a new ticket with no reference to the notice.
The cause and how it got in	"Redis was open to the internet without a password." "Weak root password over SSH; login from IP X at DATE."	"We were attacked." "We do not know."
What you found and removed	The process, the file path, the cron job, the service, the user or the SSH key that were not yours.	"We cleaned the server."
What you did so it does not happen again	Updated, closed the port, changed passwords, moved to SSH keys, or reinstalled and restored a clean copy.	"We will be more careful."
How you confirmed it stopped	The command you used and the time (in UTC) since which you no longer see the traffic in the notice.	Nothing: without it, the provider cannot tell whether it stopped.

➞ Preparing and sending the report

- 1 **Reread the log in the notice:** the time (in UTC), the ports and the destinations tell you what to look for. Each kind of notice is explained in **an abuse notice about your server**.
- 2 **Investigate and keep timed notes** as you work: what you saw, what you copied, what you deleted. The steps are in **is my VPS compromised?**.
- 3 **Close the way in before writing “fixed”:** update, close the port in the firewall, change passwords. Without this, the report does not hold up.
- 4 **Fill in the template below** with short sentences and facts. If you did not find the cause, say so, and say what you did as a precaution (for example, reinstalling).
- 5 **Reply in the same support ticket** as the notice, before the deadline ends, and in the language it came in.
- 6 **If you do not have everything yet,** send what you have before the deadline and say what is still missing. A partial reply in time is worth more than a full one too late.

➞ The template

Subject: Abuse notice [notice identifier] - server [IP]

1. Cause and how it got in: [e.g. Redis open to the internet without a password on port 6379; or a weak root password over SSH, first login at DATE TIME UTC from IP X]

2. What I found and removed: [process and file path, cron jobs, services, users or SSH keys that were not mine]. I kept a copy for analysis before deleting.

3. What I did so it does not happen again: [updated the system and the application; closed the port in the firewall; changed the passwords; turned off root password login; or reinstalled and restored the copy from DATE]

4. How I confirmed it stopped: [since DATE TIME UTC there are no outgoing connections to the ports in the notice; command used]

Contact for questions: [name and phone or e-mail]

-  **Never put passwords, private keys or customer data in the report.**
Say that you changed the password, not what the new one is. And do not write that you removed the cause if you only deleted the file: if the abuse comes back after you said it stopped, the server is switched off again.

**If you do not know how it got in,**

the honest answer is "I could not determine the entry point; as a precaution I reinstalled the system, restored the copy from DATE, updated and changed every password". That is an answer that closes the case.

 NEED A HAND?

Written your report and want us to look at it first? Paste it into the support ticket for the notice.

[📄 Open a support ticket →](#) **SEE ALSO**[An abuse notice about your server: what it means, the deadline and what we need from you](#)[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](#)[How to clean up a compromised site](#)[After a hack, which backup do you restore? Choosing a clean copy](#)[Keeping your VPS or dedicated server secure: the six that matter](#)**interweb****Interweb Angola**

RLX Angola, Lda. · Group RLX Holdings

TAX ID (NIF) 500 260 5724

COMMERCIAL
REGISTRATION NO. 26464-25/250724REGISTERED OFFICE Rua Direita do Patriota, Bairro Dangereux
Belas, Luanda, AngolaCONTACT info@interweb.ao · +244 942 011 191 · www.interweb.aoOPENING HOURS Monday to Friday - 08 AM to 04 PM
Saturday & Sunday - Closed

RLX-AO-KB-2244 · v2026.10.21 · Generated on 21/10/2026 16:09

Online version of this
document