

KNOWLEDGE BASE · PUBLIC DOCUMENT

A security report about a vulnerable n8n or web app: update first, then reduce exposure

Security

CODE

RLX-MZ-KB-2260

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/2260>

A security report about a vulnerable n8n or web app: update first, then reduce exposure

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



For VPS and dedicated server customers with root access. The short answer: the report says an application on your server is answering in a **version with known security flaws**: n8n, WordPress and its plugins, a panel or another web application. It comes from a national incident response team (CERT), through our network and data centre provider. It does not mean you were attacked, but it is exactly what bots look for first. The order is: **update** to a fixed version (with a backup first), **check** whether anyone already got in, then **expose less**: take off the internet what does not need to be there, and put HTTPS and access control in front.

What the report may point to

What was found	What to do first
n8n on an old version	Back up, including the encryption key, then update: backing up n8n and updating n8n safely .
n8n published directly on port 5678, without HTTPS	Put it behind a proxy with HTTPS and close 5678 to the outside: n8n behind HTTPS on your own domain .
WordPress, a plugin or a theme with a known flaw	Update and remove what is abandoned: updating themes and plugins, abandoned plugin or old PHP .
A panel or management application (WHMCS, phpMyAdmin, a CMS)	Update and close the admin area to anyone who does not need it: securing WHMCS .
An application in a Docker container	Pull the fixed image and recreate the container, keeping the volumes: updating a Docker application .

➔ Dealing with the report

1 Identify what is flagged: the IP, the port and, if given, the flaw's code (a CVE). See what answers on that port: `sudo ss -tlnp`

```
docker ps --format "table {{.Names}}\t{{.Image}}\t{{.Ports}}"
```

2 Check the installed version and compare it with the fixed version in the vendor's security advisory. n8n in Docker: `docker exec CONTAINER_NAME n8n --version`. WordPress, with WP-CLI: `wp core version`

```
wp plugin list --update=available
```

3 Back up before updating: for n8n, the data folder and the encryption key; for a site, the files and the database.

4 Update. n8n with Docker Compose: `docker compose pull`
`docker compose up -d` If `docker-compose.yml` pins a version in the image, change the tag to the fixed version first. Check the version afterwards. For a WordPress site, follow **updating themes and plugins without breaking anything**.

5 Check whether it was already used: in n8n, users you did not create, new or changed workflows (especially with nodes that run commands on the server), new credentials, executions at odd hours. On the server, unknown processes and cron jobs: **is my VPS compromised?**. On a site: **spotting the risks on your site**.

6 Expose less: what only your team uses does not need to be open to everyone. For n8n, close the direct port and serve it only through the HTTPS proxy; limit the editor by IP or VPN, leaving out the webhook paths that outside services call. Details in **securing n8n**.

7 Reply to the support ticket in My Interweb, 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**. Include the version before and after.

**Do not update n8n without the encryption key saved:**

If it is lost when the container is recreated, the stored credentials can no longer be opened. Jumping several versions at once can bring changes that break workflows: read the release notes and test the main flows afterwards. If you find signs of a break-in, change every credential n8n held (API keys, e-mail passwords). If you find signs that someone already got in, closing the port is not enough: the safest path is to **reinstall the server and restore a clean copy (which backup to restore)**. Cleaning up in place is for people who know exactly what they are doing.

**System updates do not update everything:**

`Apt upgrade` (**updating a Debian or Ubuntu VPS**) does not touch applications in Docker or WordPress plugins. Each has its own way to update, and the next report is avoided by following each vendor's security advisories. 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?

Received a vulnerable application report and not sure which application it is? 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](#)[Updating n8n safely](#)[Securing n8n: access, credentials and exposed webhooks](#)[Updating themes and plugins without breaking anything](#)[Is my VPS compromised? Checking processes, cron jobs, users, SSH keys and temporary folders](#)



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



Online version of this document

RLX-MZ-KB-2260 · v2026.10.21 · Generated on 21/10/2026 20:41