interweb

Generated on 16/10/2026 16:41

KNOWLEDGE BASE · PUBLIC DOCUMENT

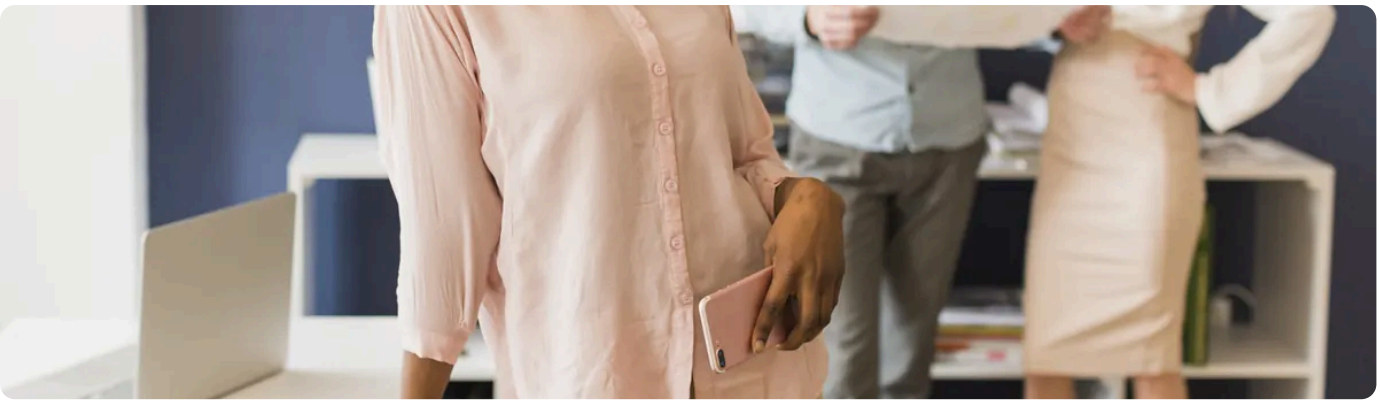
An API key or token has leaked: what to do, in the right order

Automation & n8n

CODE	VERSION	COUNTRY · LANGUAGE
RLX-MZ-KB-2170	v2026.10.16	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/2170



The short answer: if an API key, a token or a webhook secret has turned up somewhere it should not (a public repository, a file inside the site, a screenshot, an e-mail, a chat), treat it as stolen. **Revoke it and create another, before anything else.** Deleting the message or the file is not enough, because the secret may already have been copied. Then check whether anyone used it, and close the gap it got out through. This is for anyone running a site or an application connected to payments, SMS, AI, e-mail or cPanel itself.

Where secrets usually end up in plain sight

Where	Why it matters
In a Git repository, even if you deleted it in the next commit	The history keeps every version. Programs crawl public repositories looking for keys.
In the site's JavaScript or HTML	Any visitor can see it in the page source.
In a .env, a copy (.bak, .old, .zip) or a .sql dump inside the public folder	Guessing the file name is enough. See **files that must never be public**.
In error logs, or on error pages with debug mode on	Some error messages print the configuration or the request headers, key included.
In screenshots, videos, e-mails, chats and support tickets	They are stored in places you do not control, and they get forwarded.

What to do, in this order

1. **Revoke or rotate the secret in the service's dashboard** (payment operator, SMS, AI, e-mail). If the service allows two active keys, create the new one, put it in the application and revoke the old one straight after. If it does not, revoke now and accept that the integration stops until the new one is in. For cPanel tokens, see **cPanel API tokens**.

2 **Put the new secret in the right place:** an environment variable or a file outside the public folder. See **environment variables and secrets** and **keeping passwords out of your PHP code**.

3 **Review what was done with it.** In the service's dashboard, look for requests, spending, messages, payments or refunds you do not recognise since the moment the secret was exposed. If you find any, contact the service with those dates.

4 **Change whatever sat next to it.** The same file usually also holds the database password, the SMTP password and the webhook secret. If the whole file was exposed, change everything in it.

5 **Close the gap.** Move the file out of the public folder or block it, and add your secret files to `.gitignore` before the next commit: `.env` `*.env` `config/secrets.php` To find which commits contain the key, search the history for part of it: `git log -p -S "PART_OF_THE_KEY" --all` Cleaning the history helps, but it does not replace the first step.

6 **Limit the damage next time:** one key per project, with the minimum permissions, spending limits and, if the service allows it, a restriction to the IP addresses that may use it. That way revoking one does not stop the others.

Do not keep using the old secret “because nobody will have seen it”. Hunting for exposed keys is automatic and constant, on public repositories and on websites. And never paste the new secret into a support ticket, an e-mail or a chat: whoever needs to put it in the application reads it from the service’s dashboard.

If the key came out of a file that only existed on the server, the question becomes how someone got there. Changing the key is not enough: see **how to tell if your site has been compromised**.

Need help finding where the secret was exposed on your hosting? Open a ticket saying which file or folder it was in, without pasting the secret.

Open a support ticket

SEE ALSO

Environment variables and secrets for your application

Keeping passwords out of your PHP code: .env files and the right permissions

Files that must never be public: .git folders, .env, backups and database dumps

cPanel API tokens: automating without handing over your password

Getting an API key for an AI model, and keeping it safe

How to tell if your site has been compromised

interweb

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	37,000+	130+
FOUNDED	CLIENTS	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

RLX-MZ-KB-2170 · v2026.10.16 · Generated on 16/10/2026 16:41