Mozout

Gerado a 21/10/2026 17:50

BASE DE CONHECIMENTO · DOCUMENTO PÚBLICO

Uma chave de API ou um token ficou exposto: o que fazer, pela ordem certa

Automação e n8n

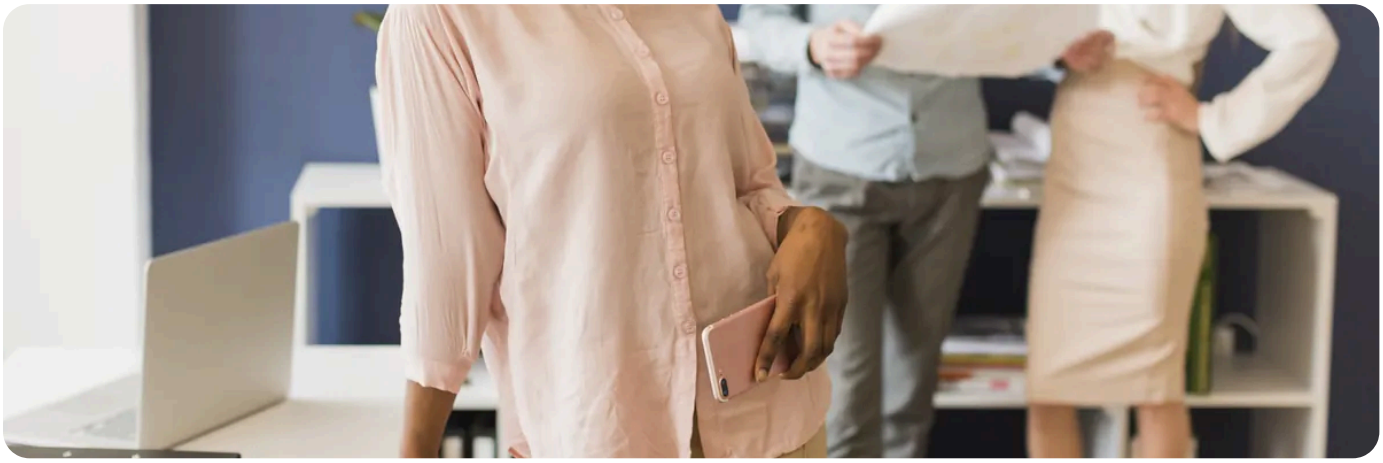
CÓDIGO	VERSÃO	PAÍS · IDIOMA
RLX-PT-KB-6594	v2026.10.16	Portugal · Português

MozOut Portugal
RLX Holdings (Pty) Ltd. · Grupo RLX Holdings
N.º fiscal (SARS) 943 907 6234 · N.º de registo (CIPC) 2025/667953/07

https://www.my.mozout.com/knowledgebase/6594

Uma chave de API ou um token ficou exposto: o que fazer, pela ordem certa

Automação e n8n Criado em **16 de outubro de 2026** 4 min de leitura



A resposta curta: se uma chave de API, um token ou o segredo de um webhook apareceu onde não devia (um repositório público, um ficheiro dentro do site, uma captura de ecrã, um e-mail, uma conversa), trate-o como roubado. **Revogue-o e crie outro, antes de tudo o resto.** Apagar a mensagem ou o ficheiro não chega, porque o segredo já pode ter sido copiado. Depois veja se alguém o usou e feche o buraco por onde saiu. Para quem gere um site ou uma aplicação ligada a pagamentos, SMS, IA, e-mail ou ao próprio cPanel.

Onde os segredos costumam ficar à vista

Onde	Porque é grave
Num repositório Git, mesmo que o tenha apagado no envio seguinte	O histórico guarda todas as versões. Há programas que percorrem os repositórios públicos à procura de chaves.
No JavaScript ou no HTML do site	Qualquer visitante o vê no código-fonte da página.
Num .env, numa cópia (.bak, .old, .zip) ou num dump .sql dentro da pasta pública	Basta adivinhar o nome do ficheiro. Veja **os ficheiros que nunca devem ser públicos**.
Em registos de erros ou em páginas de erro com o modo de depuração ligado	Algumas mensagens de erro mostram a configuração ou os cabeçalhos do pedido, com a chave lá dentro.
Em capturas de ecrã, vídeos, e-mails, conversas e pedidos de suporte	Ficam guardados em sítios que não controla, e são reencaminhados.

O que fazer, por esta ordem

1. **Revogue ou rode o segredo no painel do serviço** (operador de pagamentos, SMS, IA, e-mail). Se o serviço deixa ter duas chaves activas, crie a nova, ponha-a na aplicação e revogue a antiga logo a seguir. Se não deixa, revogue já e aceite que a integração pára até pôr a nova. Para os tokens do cPanel, veja **os tokens de API do cPanel**.

2. **Ponha o segredo novo no sítio certo:** numa variável de ambiente ou num ficheiro fora da pasta pública. Veja **variáveis de ambiente e segredos** e **tirar as palavras-passe do código PHP**.

3. **Reveja o que foi feito com ele.** No painel do serviço, procure pedidos, gastos, mensagens, pagamentos ou reembolsos que não reconhece, desde o momento em que o segredo ficou exposto. Se encontrar, contacte o serviço com essas datas.

4. **Troque também o que estava ao lado.** No mesmo ficheiro costumam estar a palavra-passe da base de dados, a do SMTP e o segredo dos webhooks. Se foi o ficheiro inteiro que ficou à vista, troque tudo o que lá estava.

5. **Feche o buraco.** Tire o ficheiro da pasta pública ou bloqueie-o, e ponha os ficheiros de segredos no `.gitignore` antes do próximo envio: `.env` `*.env` `config/secrets.php` Para saber em que envios a chave aparece no histórico, procure por um pedaço dela: `git log -p -S "PART_OF_THE_KEY" --all` Limpar o histórico ajuda, mas não substitui o primeiro passo.

6. **Reduza o estrago da próxima vez:** uma chave por projecto, com as permissões mínimas, limites de gasto e, se o serviço deixar, restrição aos endereços IP que a podem usar. Assim, revogar uma não pára as outras.

Não continue a usar o segredo antigo «porque ninguém deve ter visto».
A procura de chaves expostas é automática e constante, em repositórios públicos e em sites. E nunca cole o segredo novo num pedido de suporte, num e-mail ou numa conversa: quem precisa de o pôr na aplicação lê-o do painel do serviço.

Se a chave saiu de um ficheiro que só existia no servidor,
a pergunta passa a ser como é que alguém lá chegou. Trocar a chave não chega: veja **como saber se o site foi comprometido**.

PRECISA DE AJUDA?

Precisa de ajuda para descobrir onde o segredo ficou exposto no seu alojamento? Abra um pedido a dizer qual era o ficheiro ou a pasta, sem colar o segredo.

Abrir pedido de suporte →

VEJA TAMBÉM

- Variáveis de ambiente e segredos da sua aplicação
- Manter as palavras-passe fora do código PHP: ficheiros .env e as permissões certas
- Ficheiros que nunca devem ficar públicos: pastas .git, .env, cópias e despejos da base de dados
- Tokens de API do cPanel: automatizar sem dar a palavra-passe
- Obter uma chave de API de um modelo de IA e guardá-la em segurança
- Como saber se o meu site está infectado por malware

Mozout

MozOut Portugal

RLX Holdings (Pty) Ltd. · Grupo RLX Holdings

N.º FISCAL (SARS)	943 907 6234
N.º DE REGISTO (CIPC)	2025/667953/07
SEDE	72 York Road, Kensington Joanesburgo 2094, Gauteng, África do Sul
CONTACTOS	info@mozout.com · +27 78 823 3325 · www.mozout.com
HORÁRIO	2ª. à 6ª. Feira - 08 à 16 Horas Sábado & Domingo - Fechado

Versão online deste documento

RLX-PT-KB-6594 · v2026.10.16 · Gerado a 21/10/2026 17:50