interweb

Gerado a 16/10/2026 16:40

BASE DE CONHECIMENTO · DOCUMENTO PÚBLICO

Proteger o WHMCS: pasta da administração, dois factores, permissões e actualizações

Escolher o plano certo

CÓDIGO	VERSÃO	PAÍS · IDIOMA
RLX-MZ-KB-2122	v2026.10.16	Moçambique · Português

Interweb Moçambique
RLX Holdings, S.A. · Grupo RLX Holdings
NUIT 401 191 607 · NUEL 105 045 974 · CAE 62022

https://www.meu.interweb.co.mz/knowledgebase/2122

Este artigo é para quem revende hospedagem e tem o seu próprio WHMCS. O WHMCS é um produto de outra empresa: não vendemos nem revendemos licenças, como se explica em ***o que é o WHMCS****. Os nomes dos menus são os do WHMCS em inglês e mudam de versão para versão.* **A resposta curta:** um WHMCS guarda os dados dos seus clientes, as facturas e as chaves que criam e apagam contas no WHM. Protege-se em cinco frentes: a **pasta da administração** com outro nome, **dois factores** em todos os administradores, o **ficheiro de configuração** só de leitura, as **pastas que escrevem** fora da parte pública, e **actualizações** em dia, sempre com cópia antes.

O que proteger, e porquê

Peça	O risco se ficar como vem
A pasta `admin`	É o primeiro endereço que os robôs experimentam. Com o nome de origem, qualquer pessoa sabe onde está a porta.
As contas de administrador	Uma palavra-passe roubada abre tudo: clientes, facturas e a chave do WHM. Sem segundo factor, não há segunda barreira.
O ficheiro `configuration.php`	Tem a palavra-passe da base de dados e a chave que cifra os dados guardados. Se puder ser alterado, um ataque fica lá a morar.
As pastas onde o WHMCS escreve (anexos, transferências, modelos compilados)	Dentro da parte pública, um ficheiro carregado por alguém pode ser aberto pelo navegador.
A pasta `install`	Esquecida no servidor, deixa correr o instalador outra vez por cima da sua instalação.
Uma versão antiga	As falhas corrigidas pelo fabricante passam a ser públicas. Quem não actualiza fica com elas.

Os passos, por esta ordem

1. **Faça uma cópia primeiro:** ficheiros e base de dados, guardada fora da conta. Ver **fazer e guardar a sua própria cópia**.

2. **Apague a pasta** `install` se ainda existir.

3. **Mude o nome da pasta da administração.** Renomeie a pasta no Gestor de Ficheiros e diga ao WHMCS o nome novo, com esta linha no `configuration.php` (troque pelo seu nome): `$customadminpath = 'nome-que-so-voce-sabe';` Guarde o endereço novo nos favoritos: o antigo deixa de responder.

4. **Ligue os dois factores:** em **Configuration > System Settings > Two-Factor Authentication** active um método e obrigue os administradores a usá-lo. Cada administrador termina a activação no seu próprio perfil. Faça o mesmo na sua conta connosco: **activar a verificação em dois passos**.

5. **Ponha o** `configuration.php` **só de leitura** (por exemplo 400 ou 444), como o próprio ecrã de estado do WHMCS recomenda. Ver **permissões de ficheiros explicadas**.

6 **Tire da parte pública as pastas que escrevem** (anexos, transferências, modelos compilados) e, se quiser, a pasta `crons`. A documentação do WHMCS diz que linha de configuração indica o sítio novo de cada uma. Se mudar a `crons`, corrija o caminho da tarefa agendada no cPanel no mesmo minuto: **tarefas agendadas**.

7 **Abra o ecrã de estado do sistema** (System Health, no menu de utilitários) e resolva o que ele marcar como aviso.

8 **Actualize** quando sair uma versão nova, depois de confirmar que a sua licença a cobre e que a versão de PHP da pasta é suportada. Use sempre o mesmo caminho para actualizar: o actualizador do WHMCS ou o instalador de aplicações do cPanel, não os dois à vez.

Não perca o segundo factor sem um plano B. Guarde os códigos de recuperação num sítio que não seja o telemóvel. E não insista na palavra-passe quando a entrada falha: tentativas seguidas podem bloquear o seu IP, e isso já não é o WHMCS: **desbloquear o seu IP**.

Cada pessoa, o seu administrador. Não partilhe a mesma conta de administração entre colegas. Com contas separadas, dá a cada um só as permissões de que precisa e o registo de actividade diz quem fez o quê.

Suspeita que alguém entrou no seu WHMCS? Diga-nos o endereço e a hora, e vemos os registos do servidor do nosso lado.

Abrir pedido de suporte

VEJA TAMBÉM

Instalar o WHMCS na sua conta

Os problemas mais comuns no WHMCS, e o que os causa

Permissões de ficheiros explicadas: o que significam 755, 644 e 777

Ficheiros que nunca devem ficar públicos: pastas .git, .env, cópias e despejos da base de dados

Como activar ou desactivar a autenticação de dois factores (2FA)

Fazer e guardar a sua própria cópia, e testar se ela presta

interweb

Versão online deste documento

A Interweb é uma empresa líder em serviços de internet, com a missão de ajudar negócios a nascerem e prosperarem por meio da tecnologia.

2020
FUNDADA

37 mil+
CLIENTES

130+
INSCRIÇÕES POR DIA

Interweb Moçambique

RLX Holdings, S.A. · Grupo RLX Holdings

NUIT	401 191 607
NUEL	105 045 974
CAE	62022
SEDE	Bairro 7 de Setembro Vilankulo 1304 · CEP 0411-02, Inhambane, Moçambique
CONTACTOS	info@interweb.co.mz · +258 84 635 1111 · +258 86 635 1111 · www.interweb.co.mz
HORÁRIO	2ª. à 6ª. Feira - 08 à 16 Horas Sábado & Domingo - Fechado

RLX-MZ-KB-2122 · v2026.10.16 · Gerado a 16/10/2026 16:40