interweb

Gerado a 21/10/2026 16:18

BASE DE CONHECIMENTO · DOCUMENTO PÚBLICO

Relatório sobre um n8n ou aplicação web vulnerável: actualizar primeiro, depois expor menos

Segurança

CÓDIGO	VERSÃO	PAÍS · IDIOMA
RLX-AO-KB-2260	v2026.10.21	Angola · Português

Interweb Angola
RLX Angola, Lda. · Grupo RLX Holdings
NIF 500 260 5724 · Matrícula 26464-25/250724

https://www.meu.interweb.ao/knowledgebase/2260

Relatório sobre um n8n ou aplicação web vulnerável: actualizar primeiro, depois expor menos

Segurança · Criado em **21 de outubro de 2026** · 4 min de leitura

Para quem tem um VPS ou um servidor dedicado com acesso root. A resposta curta: o relatório diz que no seu servidor responde uma aplicação numa **versão com falhas de segurança conhecidas**: um n8n, um WordPress e os seus plugins, um painel ou outra aplicação web. Chega-nos de uma equipa nacional de resposta a incidentes (CERT), pelo nosso fornecedor de rede. Não quer dizer que foi atacada, mas é exactamente o que os robôs procuram primeiro. A ordem é: **actualizar** para uma versão corrigida (com cópia antes), **verificar** se alguém já entrou, e depois **expor menos**: tirar da internet o que não precisa de lá estar, e pôr à frente HTTPS e acesso controlado.

O que o relatório pode apontar

O que foi encontrado	O que fazer primeiro
n8n numa versão antiga	Cópia, incluindo a chave de encriptação, e actualizar: **cópia do n8n** e **actualizar o n8n sem sustos**.
n8n publicado directamente na porta 5678, sem HTTPS	Pôr atrás de um proxy com HTTPS e fechar a 5678 de fora: **o n8n com HTTPS no seu domínio**.
WordPress, um plugin ou um tema com falha conhecida	Actualizar e remover o que está abandonado: **actualizar temas e plugins**, **plugin abandonado ou PHP antigo**.
Um painel ou uma aplicação de gestão (WHMCS, phpMyAdmin, um CMS)	Actualizar e fechar a área de administração a quem não precisa: **proteger o WHMCS**.
Uma aplicação num contentor Docker	Puxar a imagem corrigida e recriar o contentor, sem perder os volumes: **actualizar uma aplicação Docker**.

Como responder ao relatório

1. **Identifique o que é apontado:** o IP, a porta e, se vier, o código da falha (um CVE). Veja o que responde nessa porta: `sudo ss -tlnp`
`docker ps --format "table {{.Names}}\t{{.Image}}\t{{.Ports}}"`

2. **Veja a versão instalada** e compare-a com a versão corrigida indicada no aviso de segurança do fabricante. n8n em Docker: `docker exec NOME_DO_CONTENTOR n8n --version`. WordPress, com WP-CLI: `wp core version`
`wp plugin list --update=available`

3. **Faça uma cópia antes de actualizar:** no n8n, a pasta de dados e a chave de encriptação; num site, os ficheiros e a base de dados.

4. **Actualize.** n8n em Docker Compose: `docker compose pull`
`docker compose up -d` Se o `docker-compose.yml` fixa uma versão na imagem, mude primeiro a etiqueta para a versão corrigida. Confirme a versão depois. Num site WordPress, siga **actualizar temas e plugins sem partir nada**.

5. **Verifique se já foi usada:** no n8n, utilizadores que não criou, workflows novos ou alterados (sobretudo com nós que correm comandos no servidor), credenciais novas, execuções a horas estranhas. No servidor, processos e tarefas cron desconhecidos: **o meu VPS foi invadido?**. Num site: **como descobrir os riscos do site**.

6. **Exponha menos:** o que só a sua equipa usa não precisa de estar aberto a todos. No n8n, feche a porta directa e sirva só pelo proxy com HTTPS; limite o editor por IP ou por VPN, deixando de fora os caminhos de webhook que serviços externos chamam. Pormenores em **proteger o n8n**.

7. **Responda ao pedido de suporte** no Meu Interweb, dentro do prazo do aviso (curto, muitas vezes de um dia), com um relatório curto: a causa, o que mudou e como confirmou que a porta já não responde de fora. Há um modelo em **responder a um aviso de abuso**. Sem resposta, ou se o problema continuar, o servidor pode ser desligado para proteger a rede, com os dados intactos: **porque o servidor é desligado e como o voltar a ligar**. Inclua a versão antes e depois.

Não actualize o n8n sem a chave de encriptação guardada:
Se ela se perder ao recriar o contentor, as credenciais guardadas deixam de abrir. Saltar várias versões de uma vez pode trazer mudanças que partem workflows: leia as notas da versão e teste os fluxos principais depois. Se encontrar sinais de entrada, troque todas as credenciais que o n8n guardava (chaves de API, palavras-passe de e-mail). Se encontrar sinais de que alguém já entrou, fechar a porta não chega: o mais seguro é **reinstalar o servidor e repor uma cópia limpa** (**que cópia restaurar**). A limpeza no sítio é para quem sabe o que está a fazer.

As actualizações do sistema não actualizam tudo:
O `apt upgrade` (**actualizar um VPS Debian ou Ubuntu**) não toca em aplicações em Docker nem em plugins do WordPress. Cada uma tem a sua forma de actualizar, e o próximo relatório evita-se acompanhando os avisos de segurança de cada fabricante. Num VPS o acesso root é seu: nós não entramos no servidor nem mudamos a firewall que está lá dentro. Se ficar sem SSH, diga-nos no pedido de suporte.

PRECISA DE AJUDA?

Recebeu um relatório de aplicação vulnerável e não sabe que aplicação é? Envie-nos no pedido de suporte o resultado do passo 1.

Abrir pedido de suporte →

VEJA TAMBÉM

- **Um aviso de abuso sobre o seu servidor: o que significa, o prazo e o que precisamos de si** →
- **Responder a um aviso de abuso: a causa, o que removeu e como não se vai repetir** →
- **Actualizar o n8n sem sustos** →
- **Proteger o n8n: acesso, credenciais e webhooks expostos** →
- **Actualizar temas e plugins sem partir nada** →
- **O meu VPS foi invadido? Verificar processos, cron, utilizadores, chaves SSH e pastas temporárias** →

interweb

Interweb Angola

RLX Angola, Lda. · Grupo RLX Holdings

NIF	500 260 5724
MATRÍCULA	26464-25/250724
SEDE	Rua Direita do Patriota, Bairro Dangereux Belas, Luanda, Angola
CONTACTOS	info@interweb.ao · +244 942 011 191 · www.interweb.ao
HORÁRIO	2ª. à 6ª. Feira - 08 à 16 Horas Sábado & Domingo - Fechado

Versão online deste documento

RLX-AO-KB-2260 · v2026.10.21 · Gerado a 21/10/2026 16:18