# Engenharia de Segurança

## Hands-On 1

### Kali Forms

**Eduardo Cunha PG55939**

Fevereiro 2025

## Vulnerabilidades

O software que escolhi é o Kali Forms, um plugin do WordPress. Seguem-se três vulnerabilidades registadas nos últimos 12 meses:

| Nome | Descrição |
|---|---|
| CVE-2024-22305 | Authorization Bypass Through User-Controlled Key vulnerability in kali Forms Contact Form builder with drag & drop for WordPress – Kali Forms.This issue affects Contact Form builder with drag & drop for WordPress – Kali Forms: from n/a through 2.3.36. |
| CVE-2024-1218 | The Contact Form builder with drag & drop for WordPress – Kali Forms plugin for WordPress is vulnerable to unauthorized access and modification of data via API due to an inconsistent capability check on several REST endpoints in all versions up to, and including, 2.3.41. This makes it possible for authenticated attackers, with contributor access and higher, to obtain access to or modify forms or entries. |
| CVE-2024-1217 | The Contact Form builder with drag & drop for WordPress &8211 Kali Forms plugin for WordPress is vulnerable to unauthorized plugin deactivation due to a missing capability check on the await_plugin_deactivation function in all versions up to, and including, 2.3.41. This makes it possible for authenticated attackers, with subscriber access or higher, to deactivate any active plugins. |

## CVE-2024-1217

| Campo | Descrição |
|---|---|
| ID CVE | CVE-2024-1217 |
| Descrição | O plugin Construtor de Formulários de Contacto com drag & drop para WordPress – Kali Forms é vulnerável a desativação não autorizada do plugin devido à falta de verificação de capacidades na função await_plugin_deactivation em todas as versões até e incluindo a 2.3.41. Isto possibilita que atacantes autenticados, com acesso de subscritor ou superior, desativem qualquer plugin ativo. |
| Pontuação CVSS e sua interpretação | 7.6 (Alta) |
| Categoria CWE associada | CWE-285: Autorização Indevida |
| Exploração disponível (Sim/Não) | Sim |
| Possíveis mitigações ou soluções sugeridas | Atualizar para a versão 2.3.42 ou superior, onde a falha foi corrigida. Configurar permissões de utilizador de forma mais restritiva no WordPress para evitar explorações indevidas. |

## CVE-2024-1218

| Campo | Descrição |
|---|---|
| ID CVE | CVE-2024-1218 |
| Descrição | O plugin Construtor de Formulários de Contacto com drag & drop para WordPress – Kali Forms é vulnerável a acesso não autorizado e modificação de dados através da API devido a uma verificação inconsistente de capacidades em vários endpoints REST em todas as versões até e incluindo a 2.3.41. Isto possibilita que atacantes autenticados, com acesso de contribuidor ou superior, obtenham acesso ou modifiquem formulários ou entradas. |
| Pontuação CVSS e sua interpretação | 4.3 (Média) |
| Categoria CWE associada | CWE-862: Autorização em Falta |
| Exploração disponível (Sim/Não) | Sim |
| Possíveis mitigações ou soluções sugeridas | Atualizar para a versão mais recente do plugin (2.3.42 ou superior), onde a falha foi corrigida. Limitar o acesso aos endpoints da API afetados utilizando plugins de segurança ou configurações a nível de servidor. |

## CVE-2024-22305

| Campo | Descrição |
|---|---|
| ID CVE | CVE-2024-22305 |
| Descrição | Vulnerabilidade de Bypass de Autorização Através de Chave Controlada pelo Utilizador no construtor de Formulários de Contacto com drag & drop para WordPress – Kali Forms. Este problema afeta o construtor de Formulários de Contacto com drag & drop para WordPress – Kali Forms: desde n/a até à versão 2.3.36. |
| Pontuação CVSS e sua interpretação | 7.5 (Alta) |
| Categoria CWE associada | CWE-639: Bypass de Autorização Através de Chave Controlada pelo Utilizador |
| Exploração disponível (Sim/Não) | Sim |
| Possíveis mitigações ou soluções sugeridas | Atualizar o plugin para a versão mais recente. Implementar medidas de controlo de acesso para evitar explorações através de chaves controladas pelo utilizador. |
| Qual é o impacto da vulnerabilidade num ambiente de produção? | Um atacante pode aceder a funcionalidades restritas do plugin sem a devida autorização, comprometendo a integridade dos formulários e possivelmente expondo dados sensíveis. |
| Quais sistemas poderiam ser comprometidos? | Sites que utilizem o plugin Kali Forms até à versão 2.3.36, especialmente aqueles que permitem registo de utilizadores com permissões mais baixas. |
| Quais medidas preventivas podem reduzir o risco? | Manter o plugin atualizado, utilizar plugins de segurança para reforçar a autenticação e limitar o acesso às funcionalidades do Kali Forms com regras de firewall ou configurações no servidor. |
| Há um patch disponível, e como pode ser aplicado? | Sim. A falha foi corrigida nas versões posteriores à 2.3.36. A atualização pode ser feita através do painel do WordPress em Plugins > Kali Forms > Atualizar ou descarregando manualmente do repositório oficial. |
| Se não houver patch, sugerir alternativas para mitigar o risco. | Se a atualização não puder ser aplicada de imediato, recomenda-se desativar o plugin temporariamente, restringir permissões REST API e monitorizar acessos suspeitos ao sistema. |