



# ALERTA DE VULNERABILIDADE

Vulnerabilidade do plug-in Forminator para  
WordPress **(Crítica)**

CVE-2023-4596

Receba alertas e informações sobre segurança cibernética e ameaças rapidamente, por meio do nosso Twitter.



## [Heimdall Security Research](#)



Acesse boletins diários sobre agentes de ameaças, *malwares*, indicadores de comprometimentos, TTPs e outras informações no *site* da ISH.



## [Boletins de Segurança – Heimdall](#)



ISH

### CONTAS DO FACEBOOK SÃO INVADIDAS POR EXTENSÕES MALICIOSAS DE NAVEGADORES

Descoberto recentemente que atores maliciosos utilizam extensões de navegadores para realizar o roubo de cookies de sessões de sites como o Facebook. A extensão maliciosa é oferecida como um anexo do ChatGPT...

BAIXAR



ISH

### ALERTA PARA RETORNO DO MALWARE EMOTET!

O malware Emotet após permanecer alguns meses sem operações retornou com outro meio de propagação, via OneNote e também dos métodos já conhecidos via Planilhas e Documentos do Microsoft Office...

BAIXAR



ISH

### GRUPO DE RANSOMWARE CLOP EXPLORANDO VULNERABILIDADE PARA NOVAS VÍTIMAS

O grupo de Ransomware conhecido como Cl0p está explorando ativamente a vulnerabilidade conhecida como CVE-2023-0669, na qual realizou o ataque a diversas organizações e expôs os dados no site de data leaks...

BAIXAR

## Sumário

|   |                                     |   |
|---|-------------------------------------|---|
| 1 | Vulnerabilidade: CVE-2023-4596..... | 5 |
| 2 | Referências.....                    | 6 |

## Lista de Figuras

Figura 1 – Pesquisa realizada com o FOFA. .... 5

## 1 VULNERABILIDADE: CVE-2023-4596

---

Uma vulnerabilidade foi catalogada com a identificação CVE-2023-4596 na qual informou que o plug-in Forminator para o WordPress seria vulnerável a uploads arbitrários de arquivos devido à validação do tipo de arquivo que ocorre após o upload de um arquivo para o servidor na função “upload\_post\_image()” em versões até 1.24.6.

Isso possibilita que invasores não autenticados carregem arquivos arbitrários no servidor do site afetado, o que pode possibilitar a execução remota de código.

**Vetor:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

**Base de Pontuação:** **9,8 (crítico)**

Realizada a pesquisa foi identificado a existência de um exploit para a referida vulnerabilidade, cujo exploit teria sido criado em **20 de julho de 2023**.

Além disso, a equipe de inteligência realizou pesquisas visando identificar possíveis ativos/sites que utilizam o plug-in Forminator em sua estrutura, sendo localizado através do FOFA, **396 sites** apenas no Brasil, sendo que tais sites caso estejam na versão indicada poderão estar vulneráveis a exploração.



Figura 1 – Pesquisa realizada com o FOFA.

De acordo com as pesquisas realizadas, é altamente recomendado que os usuários do plug-in realizem a atualização para a versão 1.25.0 ou a mais recente, a qual poderá abordar a correção da vulnerabilidade.

## 2 REFERÊNCIAS

---

- Heimdall *by* ISH Tecnologia
- CVE-2023-4596 – [NIST](#)
- [Conjunto](#) de alterações publicado pelo WordPress para correção da vulnerabilidade na versão 1.25.0



heimdall  
security research

A DIVISION OF ISH