

TLP: CLEAR



# BOLETIM DE SEGURANÇA

Fortinet emite alerta sobre vulnerabilidade crítica no  
FortiWLM

Acesse a nossa nova comunidade através do  
WhatsApp!

## 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 ClOp 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	Sumário Executivo .....	4
2	Informações sobre a vulnerabilidade .....	5
3	Referências .....	6
4	Autores.....	6

## 1 SUMÁRIO EXECUTIVO

---

A [Fortinet](#) anunciou uma vulnerabilidade crítica no **Fortinet Wireless Manager** (FortiWLM) que pode ser explorada por invasores remotos para assumir o controle de dispositivos, permitindo a execução de códigos ou comandos maliciosos por meio de solicitações web especialmente projetadas. O FortiWLM é uma ferramenta centralizada utilizada para monitoramento, gerenciamento e otimização de redes sem fio, sendo amplamente adotada por instituições governamentais, organizações de saúde, entidades educacionais e grandes corporações.

## 2 INFORMAÇÕES SOBRE A VULNERABILIDADE

---

Identificada como [CVE-2023-34990](#), a falha é uma vulnerabilidade de travessia de caminho relativa, avaliada com uma pontuação de gravidade crítica de **9,8**. Uma vulnerabilidade de travessia de caminho relativo no FortiWLM pode ser explorada por um atacante remoto não autenticado para acessar arquivos confidenciais. Além disso, conforme descrito pelo NIST, essa falha também pode permitir que o invasor execute códigos ou comandos não autorizados, utilizando solicitações web projetadas de forma específica para explorar a vulnerabilidade.

A falha afeta as seguintes versões do produto, sendo importante que administradores e usuários revisem suas configurações e considerem a aplicação de atualizações pela Fortinet para minimizar riscos de explorações associados a essa vulnerabilidade crítica.

- *FortiWLM versões 8.6.0 a 8.6.5 (corrigido em 8.6.6 ou superior)*
- *FortiWLM versões 8.5.0 a 8.5.4 (corrigido em 8.5.5 ou superior)*

### 3 REFERÊNCIAS

---

- Heimdall *by* ISH Tecnologia
- [Fortiguard](#)
- [Bleepingcomputer](#)

### 4 AUTORES

---

- Ismael Rocha



heimdall  
security research

A DIVISION OF ISH