



ALERTA DE VULNERABILIDADE

Vulnerabilidade no Jorani anteriores a versão 1.0.2

CVE-2023-26469

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 cou 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	Vulnerabilidade: CVE-2023-26469	5
2	Referências.....	6

Lista de Figuras

Figura 1 – Pesquisa realizada pelo Shodan. 5

1 VULNERABILIDADE: CVE-2023-26469

Uma vulnerabilidade no **Jorani** anteriores a1.0.2 poderá permitir que um ator malicioso aproveite o *path traversal* para acessar arquivos e executar código no servidor.

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

De acordo com a análise da vulnerabilidade, o *exploit* desenvolvido abusa do envenenamento de log e do desvio de redirecionamento por meio de falsificação de cabeçalho e, em seguida usa o *path traversal* para acionar a vulnerabilidade.

Realizadas consultas com o **Shodan**, foi possível identificar a existência do total de **6 (seis)** servidores potencialmente vulneráveis existentes no Brasil.

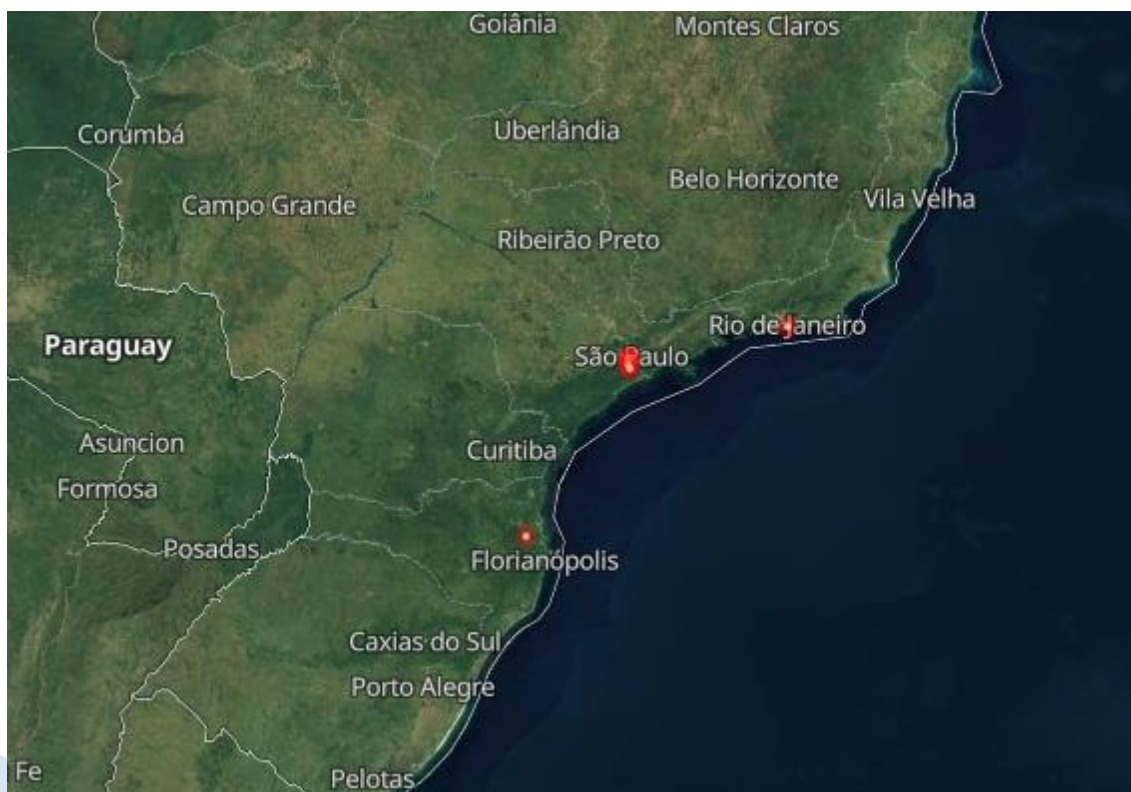


Figura 1 – Pesquisa realizada pelo Shodan.

2 REFERÊNCIAS

- Heimdall *by* ISH Tecnologia
- Jorani Remote Code Execution – [Packet Storm](#)
- CVE-2023-26469 - [NIST](#)



heimdall
security research

A DIVISION OF ISH