ALERTA DE VULNERABILIDADE

Vulnerabilidade no Jorani anteriores a versão 1.0.2

CVE-2023-26469

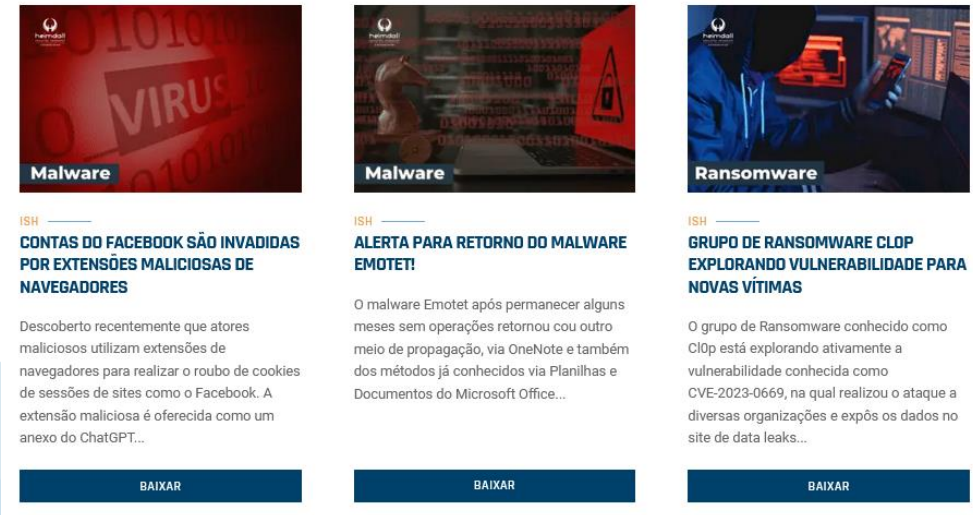
heimdall
security research
A DIVISION OF ISH

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



Sumário

Lista de Figuras

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.

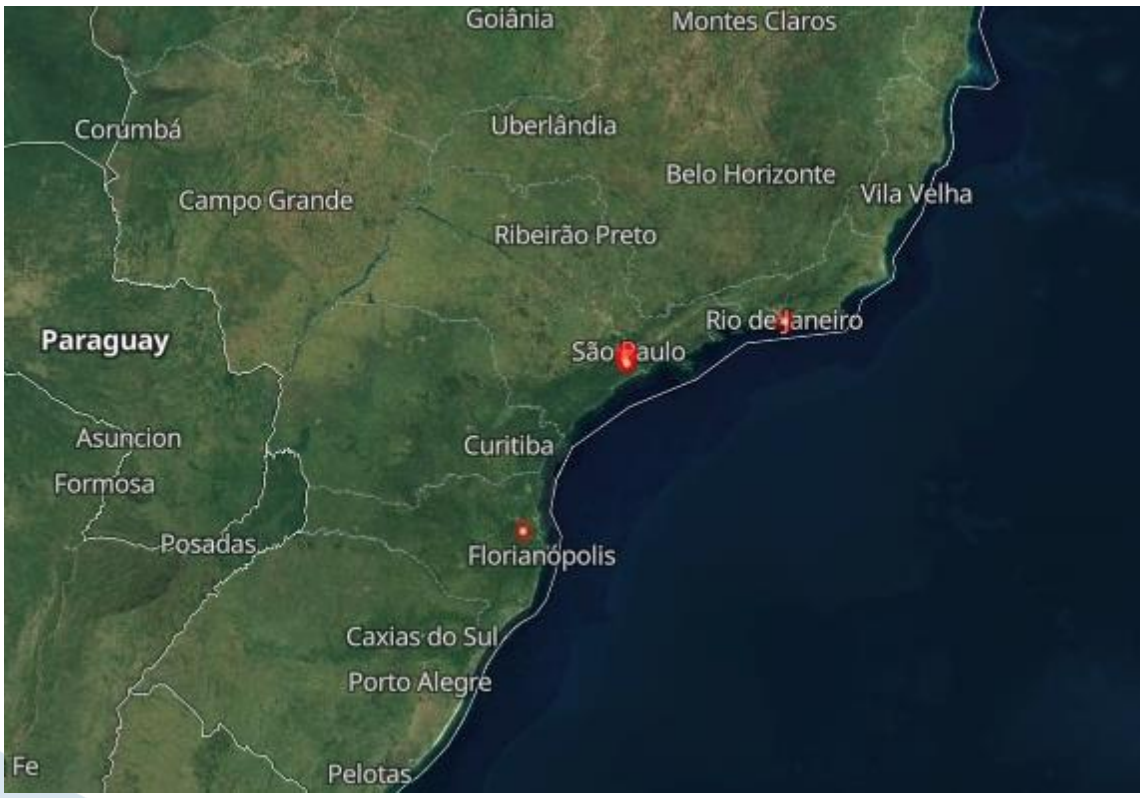


Figura 1 – Pesquisa realizada pelo Shodan.

2 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Jorani Remote Code Execution – Packet Storm**
- **CVE-2023-26469 - NIST**


heimdall
security research
A DIVISION OF ISH