ALERTA DE VULNERABILIDADE

CVE-2023-32315 - Openfire

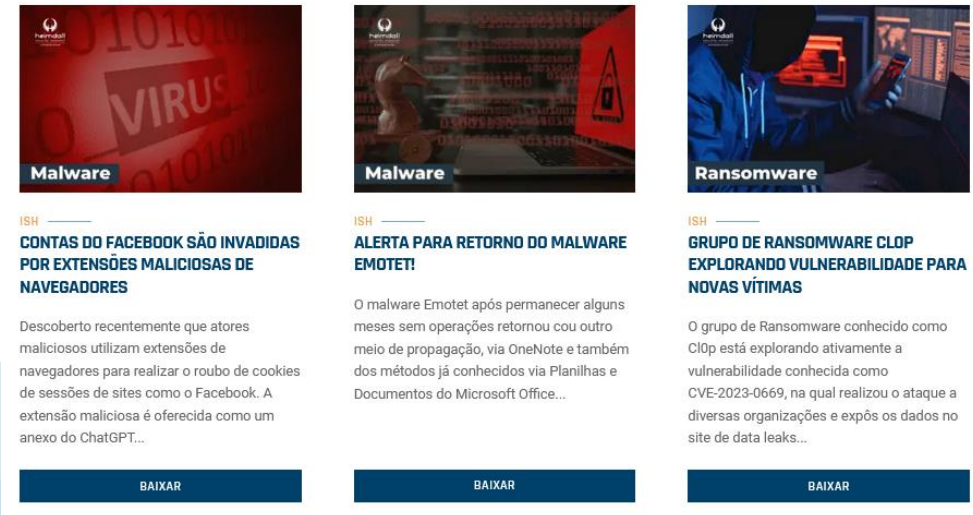
heimdall
security research
A DIVISION OF ISH

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 CVE-2023-32315 - OPENFIRE

Uma vulnerabilidade foi identificada no Openfire o qual se trata de um servidor XMPP. O console administrativo do Openfire, um aplicativo baseado na web foi considerado vulnerável a um ataque de "path traversal" através do caminho do ambiente de configuração. Isso pode permitir que um usuário não autenticado usasse o Openfire Setup Environment não autenticado em um ambiente Openfire já configurado par acessar páginas restritas no Openfire Admin Console os quais são reservados para usuários. Esta vulnerabilidade afeta todas as versões do Openfire lançadas desde abril de 2015, começando com a versão 3.10.0. A vulnerabilidade foi corrigida nas versões 4.7.5 e 4.6.8 do Openfire, e melhorias adicionais seriam incluídas na primeira versão ainda a ser lançada (4.8).

É **recomendado que seja realizada a atualização** e, se caso a atualização não estiver disponível para uma versão específica, os usuários poderão consultar o comunicado vinculado do GitHub (HSA-gw42-f939-fhvm) para obter conselhos de mitigação.

Base de pontuação da vulnerabilidade: 7,5 alto.

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

No cenário Brasileiro, é possível verificar a existência de 1.048 servidores utilizando-se do serviço Openfire, bem como a maioria dos servidores consultados possuam a utilização de versões vulneráveis do servidor.

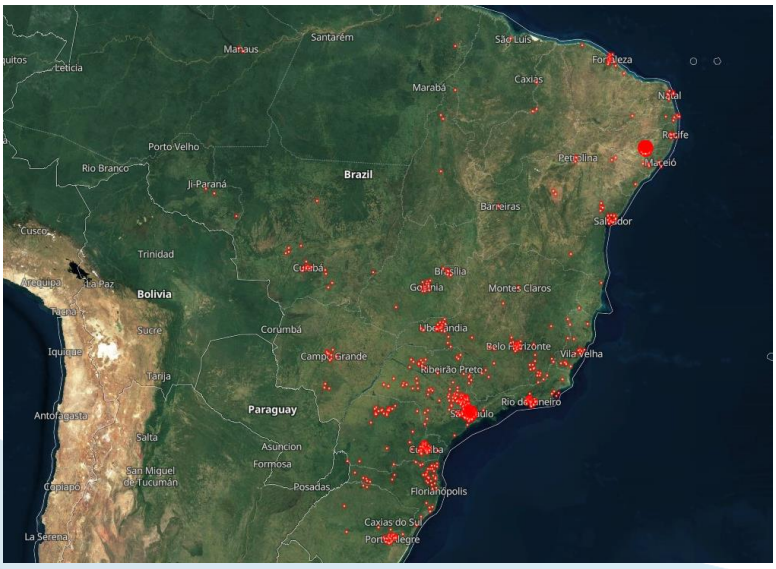


Figura 1 – Consulta ao cenário brasileiro da CVE-2023-32315.

2 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **NIST-2023-32315 - Openfire**


heimdall
security research
A DIVISION OF ISH