



ALERTA DE VULNERABILIDADE

CVE-2023-32315 - Openfire

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	CVE-2023-32315 - Openfire	5
2	Referências.....	6

Lista de Figuras

Figura 1 – Consulta ao cenário brasileiro da CVE-2023-32315. 5

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 para 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 possuem a utilização de versões vulneráveis do servidor.

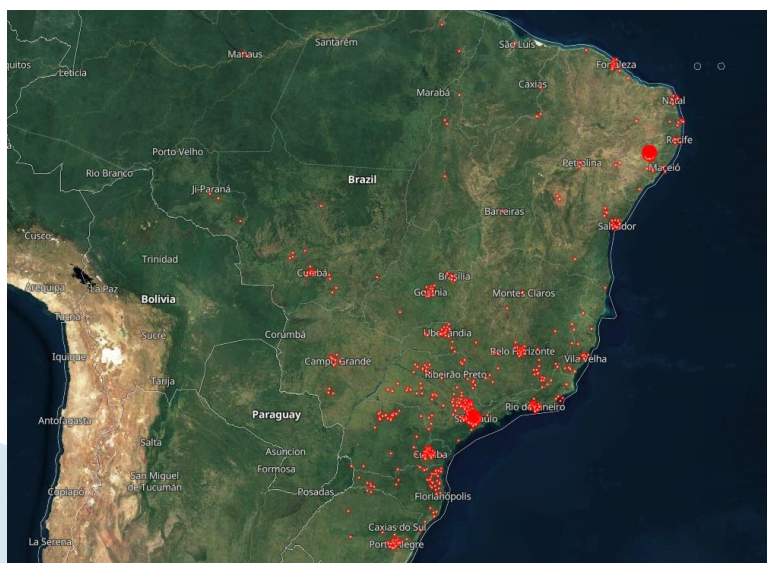


Figura 1 – Consulta ao cenário brasileiro da CVE-2023-32315.

2 REFERÊNCIAS

- Heimdall *by* ISH Tecnologia
- [NIST-2023-32315](#) - Openfire



heimdall
security research

A DIVISION OF ISH