TLP: CLEAR

BOLETIM DE SEGURANÇA

Detalhes da vulnerabilidade no Zimbra

CVE-2024-45519

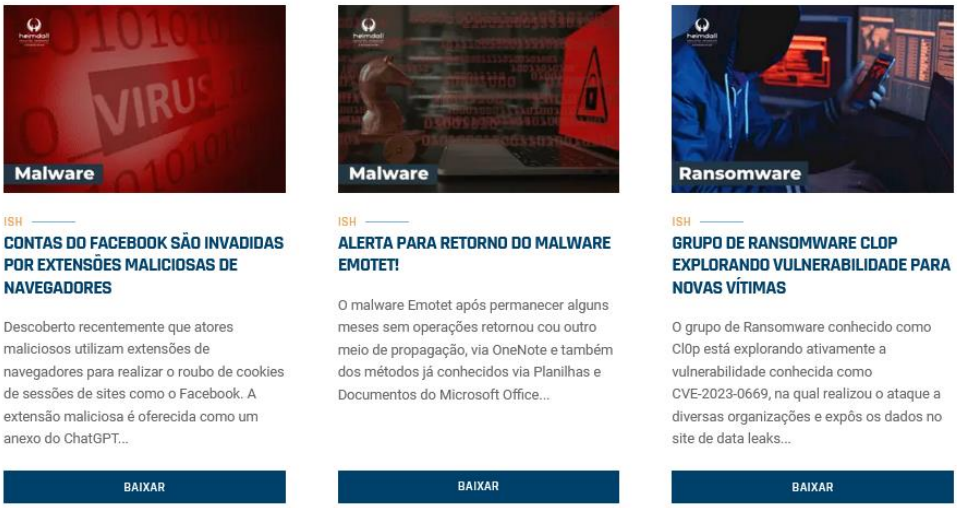
heimdall
security research
A DIVISION OF ISH

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



SUMÁRIO

LISTA DE TABELAS

LISTA DE FIGURAS

1 SOBRE A VULNERABILIDADE

Uma vulnerabilidade foi identificada como sendo potencialmente explorável por atores de ameaças em **servidores de e-mail Zimbra**. A vulnerabilidade rastreada como **CVE-2024-45519**, se encontra no servidor Zimbra utilizado por organizações de médio e grande porte, a qual pode ocasionar a execução de remota de código RCE (*Remote Code Execution*).

Quando um administrador altera manualmente as configurações padrões para ativar o serviço "***postjournal***", os invasores podem executar comandos enviando e-mails formados maliciosamente para um endereço hospedado no servidor.

A Zimbra teria corrigido recentemente esta vulnerabilidade, publicando o comunicado através de seu site.

Além disto, na terça-feira (02), um pesquisador de segurança teria relatado ataques em estado selvagem (exploração em massa) da referida vulnerabilidade. Os e-mails maliciosos estavam sendo enviados pelo endereço de IP 79.124[.]49.86 e, quando bem-sucedidos, tentam executar um arquivo hospedado usando a ferramenta "**curl**".

Na quarta-feira (03), pesquisadores relataram que o arquivo em questão não faz nada e que, o payload não é entregue por meio de uma conexão direta com o servidor malicioso por meio de SMTP. Em outra pesquisa, desta vez compartilhada pela Proofpoint, afirmava que os ataques provavelmente não levariam a infecções em massa que poderiam instalar ransomware ou malware com foco em espionagem, acrescentando ainda que existe uma PoC disponível que pode ser usada em face da vulnerabilidade.

Adicionalmente, alguns dos e-mails maliciosos utilizavam vários endereços de e-mail que, quando colocados em campo "CC", tentavam instalar um backdoor baseado em webshell em servidores Zimbra. A lista de CC completa foi agrupada em uma única string e codificada usando o base64. Quando combinados e decodados, eles criaram um webshell no path: **/jetty/webapps/zimbraAdmin/public/jsp/zimbraConfig.jsp**.

Apesar dos fatos identificados sobre a vulnerabilidade em questão (CVE-2024-45519) ser, potencialmente utilizável por atores de ameaças para fins de ataques cibernéticos, é importante que os usuários do Zimbra realizem a instalação do patch assim que possível.

2 QUANTITATIVO DE SERVIDORES

A ISH Tecnologia, realizou a pesquisa visando identificar potencialmente a volumetria de servidores Zimbra atualmente em utilização por organizações, sendo identificado que mais de **250 mil servidores** estão sendo utilizado atualmente em todo o mundo, e que **19 mil** se encontram no Brasil.

Figura 1 – Pesquisa realizada através de Favicon com FOFA.

3 RECOMENDAÇÕES

Visando corrigir a vulnerabilidade, a Zimbra por meio de seu site oficial, publicou que seria necessário atualizar os seus servidores para as versões:

Correção da vulnerabilidade de segurança no serviço “postjournal” que pode permitir que usuários não autenticados executem comandos. CVE-2024-45519	9.0.0 Path 41 10.0.9 10.1.1 8.8.15 Path 46

Tabela 1 – Descrição de versões para atualizações e correção da vulnerabilidade.

4 IoCs

Os indicadores de comprometimento obtidos relacionados a este boletim se encontram na tabela abaixo:

IP:	79[.]124.49.86

Tabela 2 – Endereço de IP identificado como explorando a vulnerabilidade em questão.

5 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Comunicado Zimbra – Avisos de vulnerabilidades.**
- **ARS Technica IA – Exploração de vulnerabilidade no Zimbra**

6 AUTORES

- **Caique Barqueta**

heimdall
security research
A DIVISION OF ISH