# BOLETIM DE SEGURANÇA

**Vulnerabilidades no Zimbra Collaboration permitem a execução de código malicioso e a inclusão local de arquivos.**

heimdall
security research
A DIVISION OF ISH

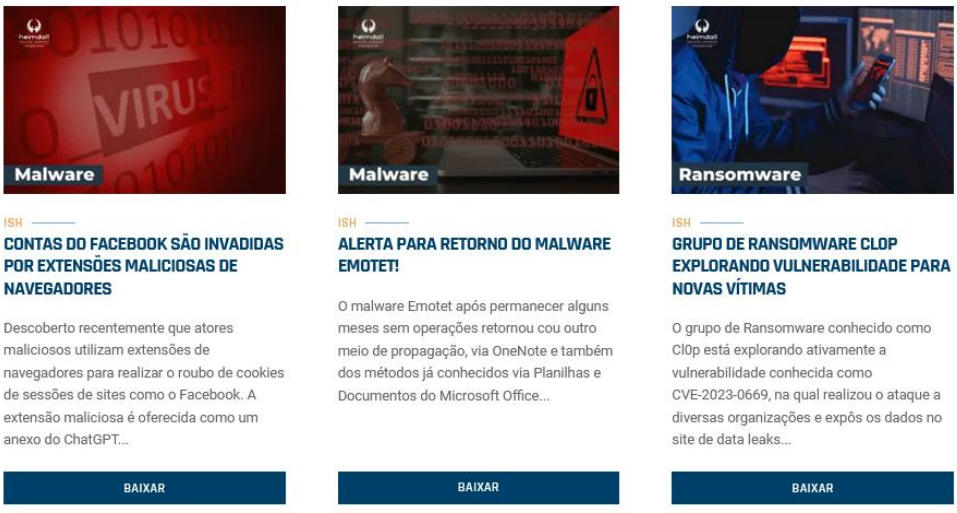
**TLP: CLEAR**

Receba alertas e informações sobre segurança cibernética e ameaças rapidamente, por meio do nosso **X**.

**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 SUMÁRIO EXECUTIVO

Recentemente foram alertadas e corrigidas três vulnerabilidades de segurança no ***Zimbra Collaboration Suite*** (ZCS), as quais destacam sérias preocupações de segurança para os administradores de sistemas que utilizam essa plataforma.

# 2 DETALHES SOBRE AS VULNERABILIDADES

Abaixo seguem os detalhes de cada uma dessas vulnerabilidades:

**CVE-2024-33533**

- **Descrição**: Descoberta no Zimbra Collaboration (ZCS) **9.0** e **10.0**, edição **1** de **2**. Uma vulnerabilidade refletida de cross-site scripting (XSS), identificada na interface de administração do webmail do Zimbra. Essa vulnerabilidade ocorre devido à validação inadequada da entrada do parâmetro packages, permitindo que um invasor autenticado injete e execute código JavaScript arbitrário dentro do contexto da sessão do navegador de outro usuário. Ao carregar um arquivo JavaScript malicioso e criar uma URL contendo sua localização no parâmetro *packages*.
- **Impacto**: Um atacante pode explorar essa vulnerabilidade para obter acesso administrativo ao sistema, permitindo a execução de comandos maliciosos, instalação de software não autorizado, ou comprometimento de dados sensíveis.

**CVE-2024-33535**

- **Descrição**: Falha de segurança descoberta no Zimbra Collaboration (ZCS) na versão **9.0** e **10.0**, esta falha envolve inclusão de arquivo local (LFI) não autenticado em um aplicativo da web, impactando especificamente o manuseio do parâmetro packages.
- **Impacto**: Os invasores podem explorar essa falha para incluir arquivos locais arbitrários sem autenticação, potencialmente levando ao acesso não autorizado a informações confidenciais. A vulnerabilidade é limitada a arquivos dentro de um diretório específico.

**CVE-2024-33536**

- **Descrição**: Falha de segurança também descoberta no Zimbra Collaboration (ZCS) na versão **9.0** e **10.0**, esta falha ocorre devido à validação de entrada inadequada do parâmetro *res*, permitindo que um invasor autenticado injete e execute código JavaScript arbitrário dentro do contexto da sessão do navegador de outro usuário. Ao carregar um arquivo JavaScript malicioso, acessível externamente, e criar uma URL contendo sua localização no parâmetro res.
- **Impacto**: Um atacante pode explorar essa vulnerabilidade para executar comandos no sistema Zimbra alvo, o que pode levar a comprometimento total do servidor.

# 3 ALERTA CTIR GOV

O Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo também fez um alerta referente as falhas de segurança Zimbra Collaboration citadas neste relatório e a importância de correções das mesmas.

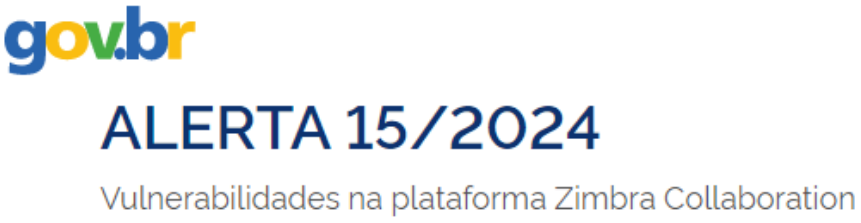



*Figura 1 – Alerta do CTIR Gov sobre as falhas no Zimbra Collaboration.*

# 4 RECOMENDAÇÕES

Abaixo são elencadas pela ISH, medidas que poderão ser adotadas visando a mitigação da referida *ameaça*, como por exemplo:

**Atualização de segurança**

- A ação mais importante é garantir que o Zimbra Collaboration Suite seja atualizado para a versão mais recente disponível que contém patches para essas vulnerabilidades.

**Segurança de rede**

- Implementar regras de firewall e sistemas de detecção de intrusão (IDS/IPS) para monitorar e bloquear tentativas de exploração dessas falhas.

**Monitoramento**

- Monitorar logs de acesso e uso do sistema para identificar comportamentos anômalos que possam indicar uma tentativa de exploração.

**Treinamento de usuários**

- Treinar os administradores e usuários na identificação de possíveis sinais de comprometimento e na aplicação das melhores práticas de segurança.

# 5 REFERÊNCIAS


- **Heimdall *by* ISH Tecnologia**
- **Zimbra**

# 6 AUTORES

- **Ismael Pereira Rocha**

heimdall
security research
A DIVISION OF ISH