



# BOLETIM DE SEGURANÇA

Microsoft realiza atualização semanal de segurança –  
**Patch Tuesday Março**



**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](#)



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 CLOP 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	Sumário Executivo .....	4
2	Detalhes das vulnerabilidades .....	5
3	Conclusão .....	6
4	Referências .....	7

## 1 SUMÁRIO EXECUTIVO

---

Recentemente a [Microsoft](#) lançou a atualização mensal de segurança, onde informa **61 falhas de segurança diferentes em seu software**. Dentre elas, dois problemas críticos afetando o **Hyper-V** que podem levar a um ataque de *denial-of-service (DoS)* e *remote code execution (RCE)*.

Das 61 vulnerabilidades, **duas delas foram caracterizadas como críticas**, 58 classificadas como importantes e uma como baixa. Essas correções, são um acréscimo de 17 falhas que foram corrigidas no navegador Edge que é baseado no Chromium em fevereiro de 2024.

## 2 DETALHES DAS VULNERABILIDADES

---

As vulnerabilidades [CVE-2024-21407](#) e [CVE-2024-21408](#), foram classificadas como críticas, pois afetam o Hyper-V, podendo resultar na execução remota de código e um ataque de negação de serviço. A atualização também mostra as falhas [CVE-2024-21400](#) de *privilege escalation* em contêiner do *Azure Kubernetes*, a falha [CVE-2024-26170](#) em sistemas de arquivos de imagem compostas do sistema e a falha [CVE-2024-21390](#) que se refere ao autenticador. Quando a exploração é bem-sucedida, exige que o invasor tenha uma presença local no dispositivo por meio de malware ou de um aplicativo malicioso já instalado por algum outro meio, sendo necessário que a vítima feche e reabra o aplicativo Authenticator. A exploração desta vulnerabilidade pode permitir que um invasor obtenha acesso a códigos de autenticação multifator (**MFA**) para as contas da vítima, podendo modificar ou excluir contas no aplicativo de autenticação, mas não impedir que o aplicativo seja iniciado ou executado. Embora essa exploração seja considerada menos provável, sabe-se que os invasores estão tentando encontrar maneiras de contornar a autenticação multifator. A vulnerabilidade [CVE-2024-21433](#) é um bug de escalonamento de privilégios no componente Print Spooler que pode permitir que um ator malicioso obtenha privilégios SYSTEM.

A atualização também corrige a falha [CVE-2024-26198](#), que se trata de uma execução remota de código no *Exchange Server*, em que um agente de ameaça não autenticado poderia exceder-se, colocando um arquivo especialmente criado em um diretório online e enganando a vítima para abri-lo, resultando na execução de arquivos DLL maliciosos. A vulnerabilidade [CVE-2024-21334](#), classificada alta, diz respeito a um caso de execução remota de código que afeta a *Open Management Infrastructure (OMI)*, em que o invasor de forma remota, não autenticado poderia acessar a instância OMI pela Internet e enviar solicitações especialmente criadas para acionar uma vulnerabilidade de uso após liberação.

### 3 CONCLUSÃO

---

A correção de segurança para essas vulnerabilidades é crucial para a proteção das organizações contra vulnerabilidades conhecidas. A mitigação de riscos, corrigindo as vulnerabilidades, reduz o risco de exploração por atacantes maliciosos. Ignorar essas correções pode resultar em violações de dados, perda financeira e danos à reputação.

## 4 REFERÊNCIAS

---

- Heimdall by ISH Tecnologia
- [Thehackernews](#)
- [Microsoft](#)



heimdall  
security research

A DIVISION OF ISH