



# BOLETIM DE SEGURANÇA

**VMware atualiza software após vulnerabilidades Zero-Days reveladas**



**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 cou 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 sobre as vulnerabilidades.....	5
3	Recomendações.....	6
4	Referências .....	7
5	Autores.....	8

## 1 SUMÁRIO EXECUTIVO

---

A VMware atualizou seus hipervisores Workstation e Fusion, corrigindo quatro falhas, das quais três foram zero-day exploradas no evento Pwn2Own Vancouver em 2024. A vulnerabilidade mais crítica, identificada como [CVE-2024-22267](#), envolvia um erro de uso após livre no vbluetooth.

## 2 DETALHES SOBRE AS VULNERABILIDADES

---

Uma delas, identificada como CVE-2024-22267, permite que atores mal-intencionados com acesso administrativo executem código no host através do processo VMX da máquina virtual. Para mitigar o risco antes das atualizações, a VMware sugere desativar o suporte Bluetooth nas configurações da máquina virtual.

Além disso, foram corrigidos dois bugs graves, [CVE-2024-22269](#) e [CVE-2024-22270](#), que possibilitavam a leitura de dados sensíveis da memória do hipervisor por usuários maliciosos com privilégios locais. A quarta falha, [CVE-2024-22268](#), relacionada a um estouro de buffer na funcionalidade Shader, poderia ser explorada para causar uma negação de serviço, mesmo sem privilégios administrativos. Essas descobertas foram reportadas pelas equipes de segurança Theori e STAR Labs SG, bem como pela Iniciativa Zero Day da Trend Micro. Para que a vulnerabilidade de segurança seja explorada com êxito, é necessário que a função de gráficos 3D esteja habilitada na máquina virtual alvo.

### 3 RECOMENDAÇÕES

---

Para administradores que não podem aplicar as [atualizações](#) de segurança imediatamente, a VMware oferece uma solução temporária. Basta desativar o suporte Bluetooth na máquina virtual, removendo a seleção da opção compartilhar dispositivos Bluetooth com a máquina virtual.

## 4 REFERÊNCIAS

---

- Heimdall by ISH Tecnologia
- [Broadcom](#)
- [Bleepingcomputer](#)
- [NVD](#)

## 5 AUTORES

---

- Leonardo Oliveira Silva



**heimdall**  
security research

A DIVISION OF ISH