BOLETIM DE SEGURANÇA

VMWare lança patches para corrigir falhas de segurança

heimdall
security research
A DIVISION OF ISH

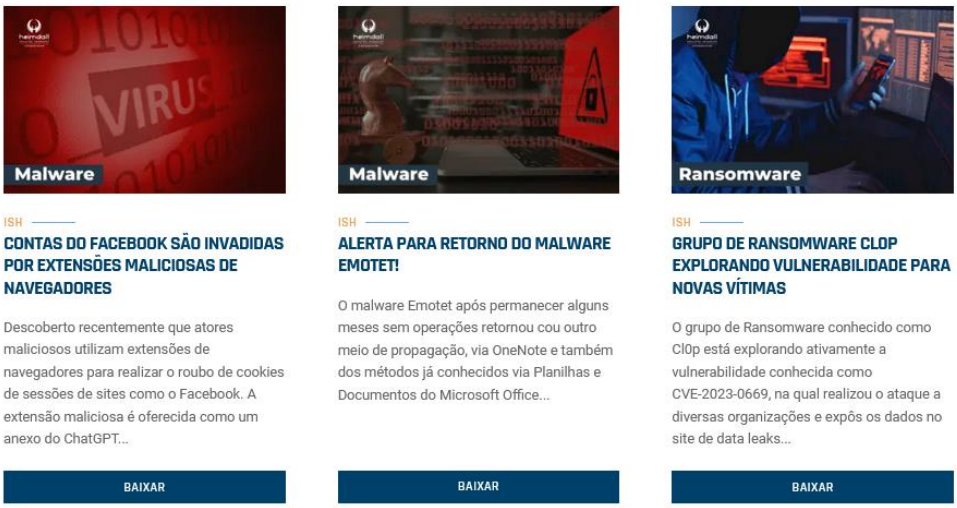
TLP: CLEAR

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

A VMware lançou patches para solucionar falhas de segurança que afetam os produtos **ESXi**, **Workstation, VMware Cloud Director** e **Fusion**, com nível críticas e alta. As vulnerabilidades, foram descritas como bugs de uso livre no controlador **USB XHCI**. Eles possuem uma pontuação. Um ator malicioso com privilégios administrativos locais em uma máquina virtual pode explorar essas falhas e executar código como o processo VMX da máquina virtual em execução no host. No ESXi, a exploração está contida na sandbox VMX, enquanto no Workstation e Fusion, isso pode levar à execução de código na máquina onde o Workstation ou Fusion está instalado.

Figura 1 – Logo da VMWare

2 DETALHES DA VULNERABILIDADE

Abaixo segue os detalhes sobre a vulnerabilidade:

Descrição

- As vulnerabilidades (**CVE-2024-22252** e **CVE-2024-22253**) são falhas de bugs livres de uso nos controladores USB XHCI e UHCI (respectivamente), impactando Workstation/Fusion e ESXi. A exploração requer privilégios administrativos locais em uma máquina virtual e pode permitir que um invasor execute código como o processo VMX da VM no host. No Workstation e no Fusion, isso pode levar à execução de código na máquina host.
- A vulnerabilidade (**CVE-2024-22254**) trata-se de uma falha de gravação fora dos limites no ESXi, permitindo que um invasor com privilégios de processo VMX grave fora da região de memória pré-determinada, potencialmente levando ao escape da sandbox.

- A vulnerabilidade (**CVE-2024-22255**) trata-se de um problema de divulgação de informações no controlador USB UHCI afetando ESXi, Workstation e Fusion. Esta vulnerabilidade pode permitir que um agente mal-intencionado com acesso administrativo a uma VM vaze memória do processo VMX.

- A falha (**CVE-2024-22256)** é uma vulnerabilidade de divulgação parcial de informações. Um ator mal-intencionado pode potencialmente coletar informações sobre nomes de organizações com base no comportamento da instância.

3 CONCLUSÃO

A importância da proteção reside na preservação da integridade dos dados. Além disso, a conformidade regulatória exige que as organizações que desejam proteger seus sistemas e dados contra vulnerabilidades conhecidas, adotando abordagens como atualização constante de sistemas de segurança e a educação dos funcionários sobre práticas seguras.

4 RECOMENDAÇÕES

Para corrigir as CVE-2024-22252, CVE-2024-22253, CVE-2024-22254, CVE-2024-22255, aplique os patches listados na coluna versão fixa' da 'Matriz de resposta, acessando o link.

Product	Version	Running On	CVE Identifier	CVSSv3	Severity	Fixed Version [1]	Workarounds	Additional Documentation
ESXi	8.0	Any	CVE-2024-22252, CVE-2024-22253, CVE-2024-22254, CVE-2024-22255	8.4, 8.4, 7.9, 7.1	Critical	ESXi80U2sb-23305545	KB96682	FAQ
ESXi	8.0 [2]	Any	CVE-2024-22252, CVE-2024-22253, CVE-2024-22254, CVE-2024-22255	8.4, 8.4, 7.9, 7.1	Critical	ESXi80U1d-23299997	KB96682	FAQ
ESXi	7.0	Any	CVE-2024-22252, CVE-2024-22253, CVE-2024-22254, CVE-2024-22255	8.4, 8.4, 7.9, 7.1	Critical	ESXi70U3p-23307199	KB96682	FAQ
Workstation	17.x	Any	CVE-2024-22252, CVE-2024-22253, CVE-2024-22255	9.3, 9.3, 7.1	Critical	17.5.1	KB96682	None.
Fusion	13.x	MacOS	CVE-2024-22252, CVE-2024-22253, CVE-2024-22255	9.3, 9.3, 7.1	Critical	13.5.1	KB96682	None

Figura 2 – Matriz de respostas vmsa-2024-0006.1

Para corrigir CVE-2024-22256, aplique os patches listados na coluna 'Versão fixa' da 'Matriz de resposta' acessando o link.

produtos	Versão	Continuando	Identificador CVE	CVSSv3	Gravidade	Versão Fixa	Soluções alternativas	Documentação Adicional
Diretor de nuvem VMware	10.5.1.1	Qualquer	CVE-2024-22256	N / D	N / D	Não afetado	N / D	N / D
Diretor de nuvem VMware	10.5.x	Qualquer	CVE-2024-22256	4.3	Moderado	10.5.1.1	N / D	N / D
Diretor de nuvem VMware	10.4.x	Qualquer	CVE-2024-22256	4.3	Moderado	10.5.1.1	N / D	N / D

Figura 3 – Matriz de respostas vmsa-2024-0007

5 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- NVD
- Thehackernews
- Bleepingcomputer
- VMWare

heimdall
security research
A DIVISION OF ISH