ALERTA DE VULNERABILIDADE

CISA adiciona uma vulnerabilidades explorada conhecida ao catálogo KEV

heimdall
security research
A DIVISION OF ISH

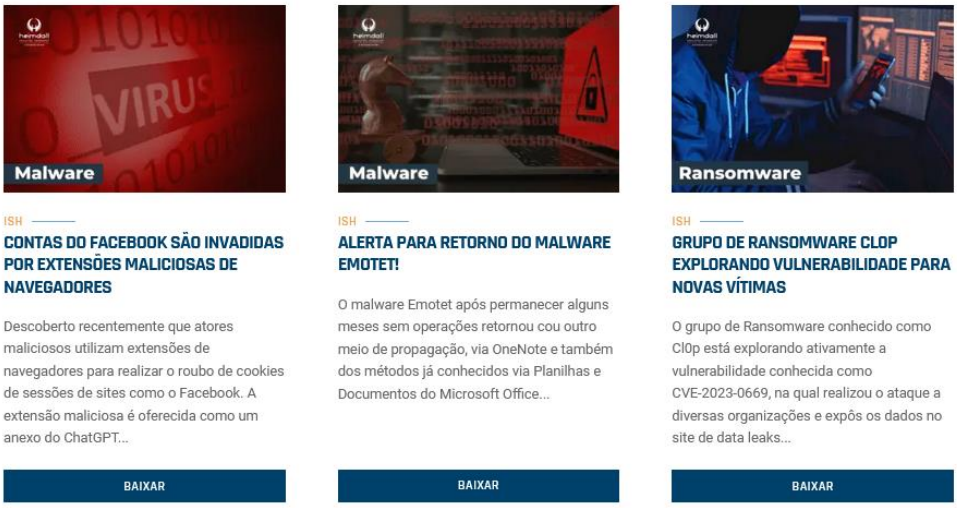
TLP: CLEAR

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

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



heimdall
security research

Sumário

Lista de Figuras

1 SUMÁRIO EXECUTIVO

Recentemente a Agência de Segurança de Infraestrutura e Cibersegurança dos EUA (CISA), anunciou a adição de **uma** nova vulnerabilidade ao seu Catálogo de Vulnerabilidades Exploradas Conhecidas (**KEV**). Essa adição é baseada em evidências de explorações ativas, pois esse tipo de vulnerabilidade são vetores de ataque frequentes para atores mal-intencionados e representa riscos significativos para as organizações.

2 VULNERABILIDADE ADICIONADA

A vulnerabilidade adicionada ao Catálogo de Vulnerabilidades Exploradas Conhecidas (KEV), é a seguinte:

CVE-2023-29360, a qual refere-se a uma vulnerabilidade de elevação de privilégios no Serviço de Streaming da Microsoft. Abaixo estão os detalhes principais:

Produtos afetados

- *Windows 10 Version 1809*
- *Windows Server 2019*
- *Windows Server 2019 (Instalação Core do Server)*
- *Windows Server 2022*
- *Windows 11 versão 21H2*
- *Windows 10 Version 21H2*
- *Windows 11 versão 22H2*
- *Windows 10 Version 22H2*
- *Windows 10 Version 1607*
- *Windows Server 2016*
- *Windows Server 2016 (Instalação Core do Server)*

Plataformas afetadas

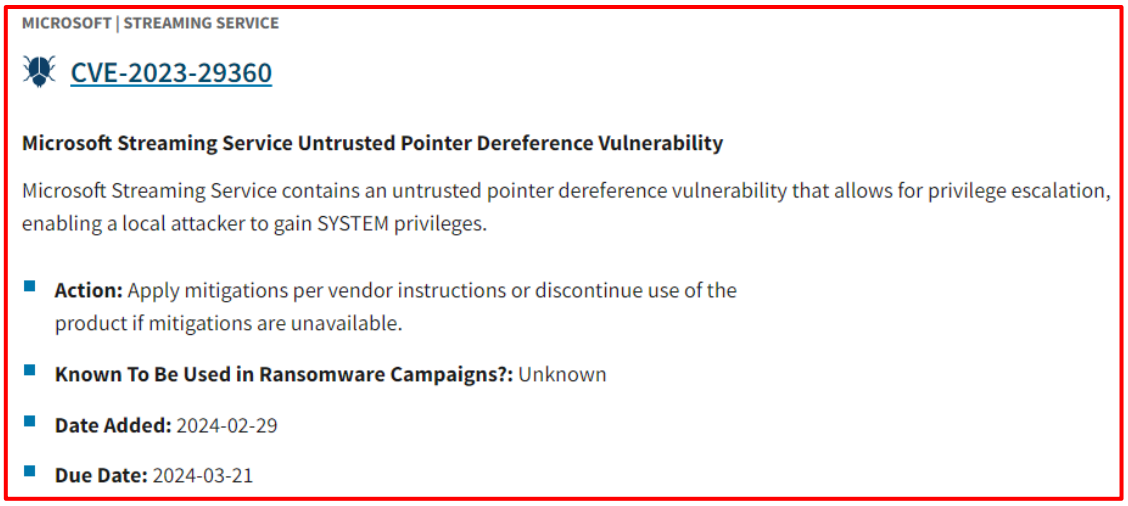
Sistemas baseados em 32 bits, x64 e ARM64.

Descrição

Esta vulnerabilidade permite a elevação de privilégios no serviço de streaming da Microsoft. Se explorada, a vulnerabilidade pode permitir que um atacante execute comandos com privilégios elevados.

Severidade

Alta, com uma pontuação CVSS 3.1 base de **8.4**. A pontuação CVSS é calculada como AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H, indicando um vetor de ataque local (AV:L), baixa complexidade de ataque (AC:L), não requer privilégios (PR:N), sem interação do usuário (UI:N), sem mudança de escopo (S:U), e impacto alto em confidencialidade (C:H), integridade (I:H), e disponibilidade (A:H).


MICROSOFT | STREAMING SERVICE

CVE-2023-29360

Microsoft Streaming Service Untrusted Pointer Dereference Vulnerability

Microsoft Streaming Service contains an untrusted pointer dereference vulnerability that allows for privilege escalation, enabling a local attacker to gain SYSTEM privileges.

- **Action:** Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.
- **Known To Be Used in Ransomware Campaigns?:** Unknown
- **Date Added:** 2024-02-29
- **Due Date:** 2024-03-21

Figura 1 – Vulnerabilidade no catálogo KEV-CISA.

Para mitigar essa vulnerabilidade, é recomendado aplicar as atualizações fornecidas pela Microsoft e seguir as orientações de segurança da empresa. A Microsoft fornece um guia de atualização específico para essa vulnerabilidade, disponível em sua página de consultoria: *Windows TPM Device Driver Elevation of Privilege Vulnerability*.

Exploração por ator de ameaça conhecida

Em fevereiro, a análise de algumas amostras do Raspberry Robin antes de outubro de 2023 revelou que os operadores também usaram um exploit para CVE-2023-29360. A exploração da vulnerabilidade CVE-2023-29360 foi divulgada publicamente em junho, e Raspberry Robin a empregou em agosto.

O acesso aos códigos de prova de conceito (PoC) possibilitou a integração de código malicioso em suas estratégias de ataque para diversos agentes de ameaça.

Figura 2 – Post no Twitter-X referente ao exploit da falha.

3 CONCLUSÃO

A correção de vulnerabilidades listadas no catálogo Vulnerabilidades Exploradas Conhecidas (KEV) da (CISA) é crucial para as organizações por várias razões. Primeiro, essas vulnerabilidades já foram exploradas ativamente por atacantes, o que aumenta o risco de incidentes de segurança se não forem corrigidas. A atenção à lista KEV permite que as organizações priorizem esforços de mitigação em vulnerabilidades comprovadamente perigosas, maximizando a eficácia da segurança cibernética.

Além disso, a conformidade com as diretrizes da CISA pode ser essencial para manter a confiança dos clientes e evitar penalidades legais, especialmente em setores regulamentados. A correção dessas vulnerabilidades também protege contra perdas financeiras significativas devido a violações de dados e interrupções operacionais. Por fim, manter-se atualizado com o catálogo KEV da CISA demonstra um compromisso com as melhores práticas de segurança cibernética, reforçando a postura de segurança geral da organização.

4 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- CISA
- KEV-CISA
- NVD
- Securityaffairs

heimdall
security research
A DIVISION OF ISH