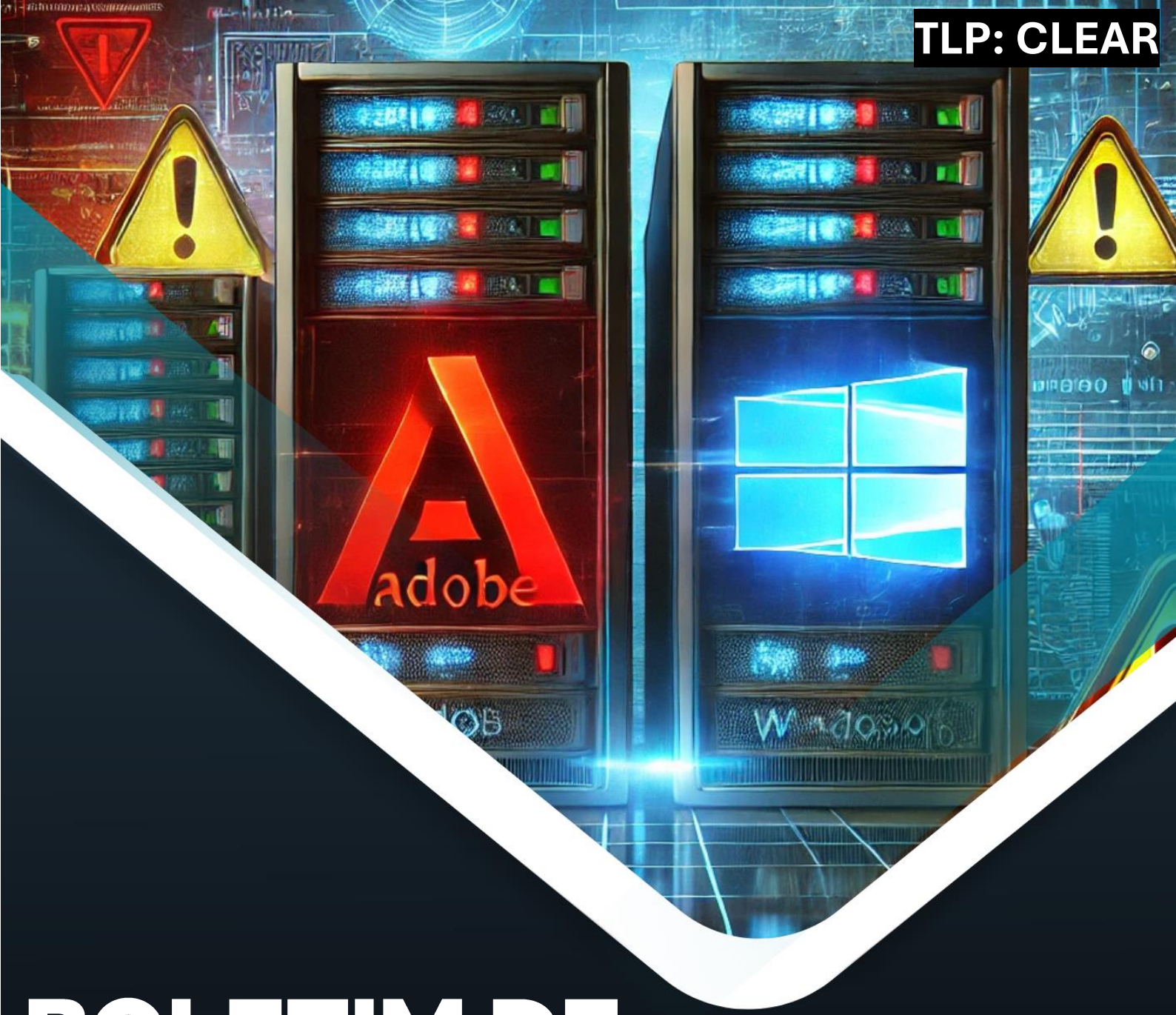
TLP: CLEAR



BOLETIM DE SEGURANÇA

CISA inclui novas vulnerabilidades ativamente exploradas em seu catálogo

heimdall
security research

Acesse a nossa nova comunidade através do WhatsApp!

Heimdall Security Research

Acesse boletins diários sobre agentes de ameaças, *malwares*, indicadores de comprometimentos, TTPs e outras informações no *site* da ISH.

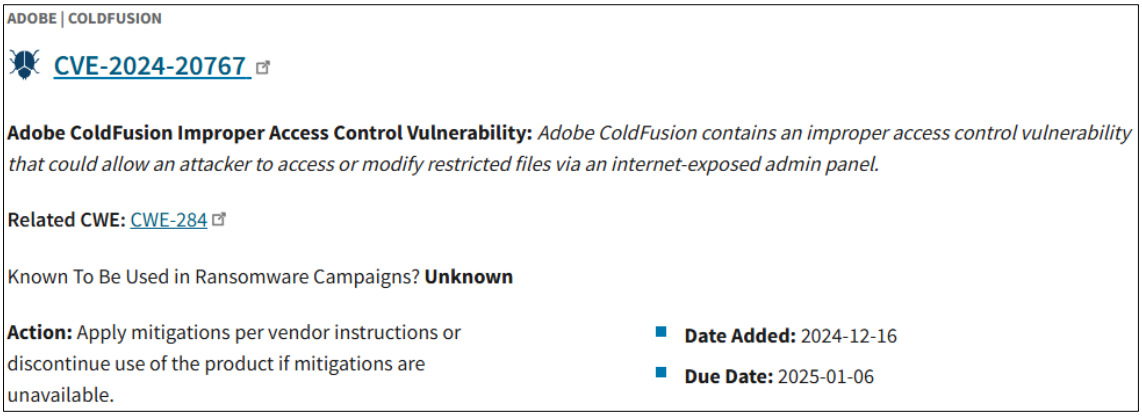
Boletins de Segurança – Heimdall

SUMÁRIO

LISTA DE FIGURAS

1 SUMÁRIO EXECUTIVO

A **Agência de Segurança Cibernética e de Infraestrutura dos Estados Unidos (CISA)** adicionou ao seu catálogo de **Vulnerabilidades Exploradas Conhecidas (KEV)** duas novas falhas de segurança. As vulnerabilidades foram detectadas nos produtos **Adobe ColdFusion** e no driver de modo kernel do **Microsoft Windows**, com a ressalva de que ambas estão sendo exploradas ativamente.


ADOBE | COLDFUSION

CVE-2024-20767

Adobe ColdFusion Improper Access Control Vulnerability: *Adobe ColdFusion contains an improper access control vulnerability that could allow an attacker to access or modify restricted files via an internet-exposed admin panel.*

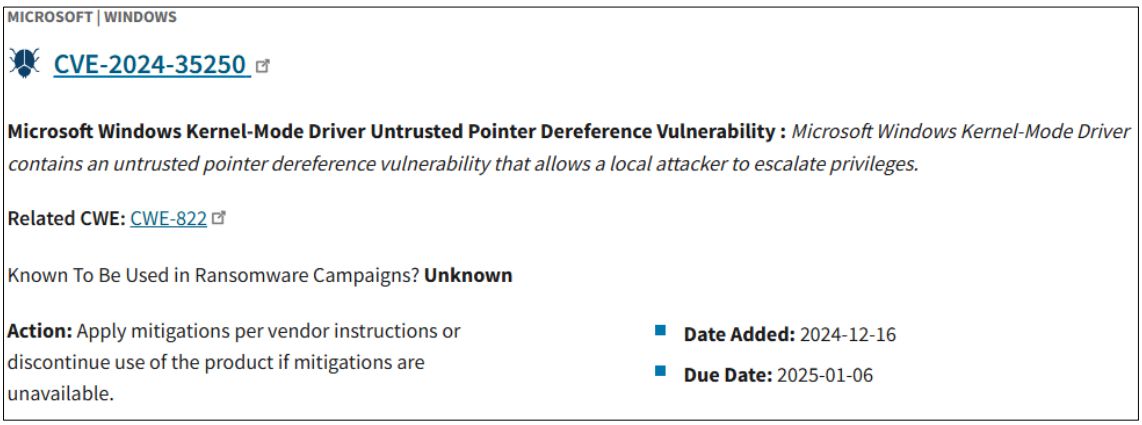
Related CWE: CWE-284

Known To Be Used in Ransomware Campaigns? **Unknown**

Action: Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.

- **Date Added:** 2024-12-16
- **Due Date:** 2025-01-06

Figura 1 – Vulnerabilidade CVE-2024-20767 no Catálogo KEV-CISA.


MICROSOFT | WINDOWS

CVE-2024-35250

Microsoft Windows Kernel-Mode Driver Untrusted Pointer Dereference Vulnerability : *Microsoft Windows Kernel-Mode Driver contains an untrusted pointer dereference vulnerability that allows a local attacker to escalate privileges.*

Related CWE: CWE-822

Known To Be Used in Ransomware Campaigns? **Unknown**

Action: Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.

- **Date Added:** 2024-12-16
- **Due Date:** 2025-01-06

Figura 2 – Vulnerabilidade CVE-2024-35250 no Catálogo KEV-CISA.

2 INFORMAÇÕES SOBRE AS VULNERABILIDADES

Segue a lista de vulnerabilidades informadas pela CISA, juntamente com uma breve descrição de cada uma:

CVE-2024-20767

As versões *2023.6*, *2021.12* e anteriores do **Adobe ColdFusion** apresentam uma vulnerabilidade relacionada a Controle de Acesso Inadequado, permitindo a leitura arbitrária do sistema de arquivos. Por meio dessa falha, um atacante pode obter acesso indevido a arquivos restritos ou até mesmo modificá-los. Vale destacar que a exploração dessa vulnerabilidade não exige interação do usuário, porém depende de o painel de administração estar exposto à Internet, facilitando o ataque.

Impacto

- Um atacante pode acessar arquivos restritos, roubando informações confidenciais.
- Há risco de modificação maliciosa de arquivos críticos do sistema.

CVE-2024-35250

Uma vulnerabilidade presente no driver de modo kernel do sistema operacional **Microsoft Windows**. Essa falha pode ser explorada para elevar privilégios no sistema, fornecendo controle avançado ao atacante e comprometendo a segurança do dispositivo.

Impacto

- A falha pode ser explorada para elevar privilégios no sistema, fornecendo controle total ao atacante.
- Com acesso privilegiado, o atacante pode instalar programas, modificar arquivos e até desativar medidas de segurança.

3 RECOMENDAÇÕES

Recomendamos fortemente que as organizações minimizem sua exposição a ataques cibernéticos, dando prioridade à rápida **correção das vulnerabilidades** como parte essencial de suas práticas de gestão de riscos e vulnerabilidades.

4 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **CISA**
- **NVD**
- **CVE**

5 AUTORES

- **Rafael de Moura Salomé**

heimdall
security research
A DIVISION OF ISH