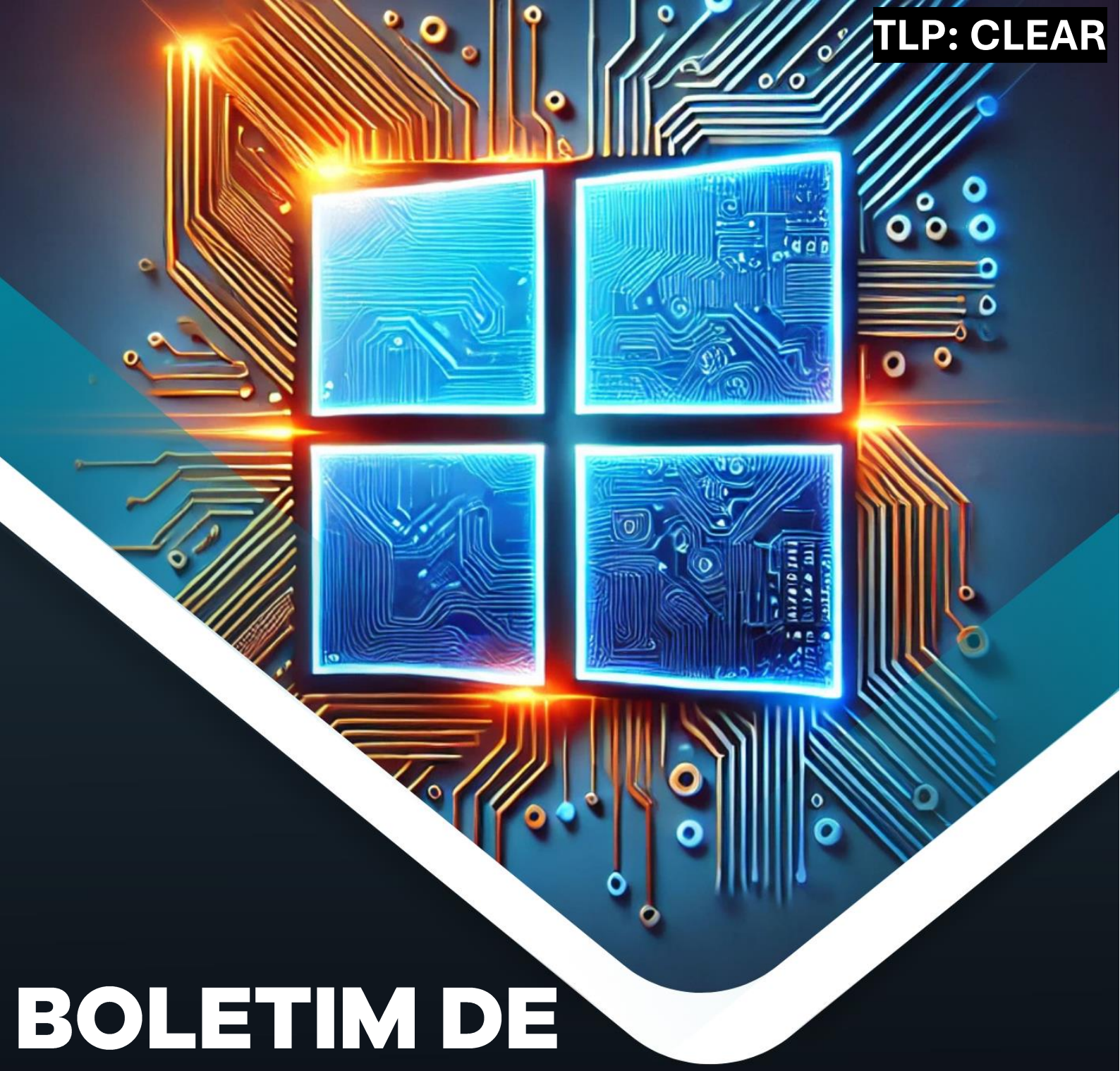
TLP: CLEAR



# BOLETIM DE SEGURANÇA

## Atualizações da Microsoft (Patch Tuesday) de outubro de 2024

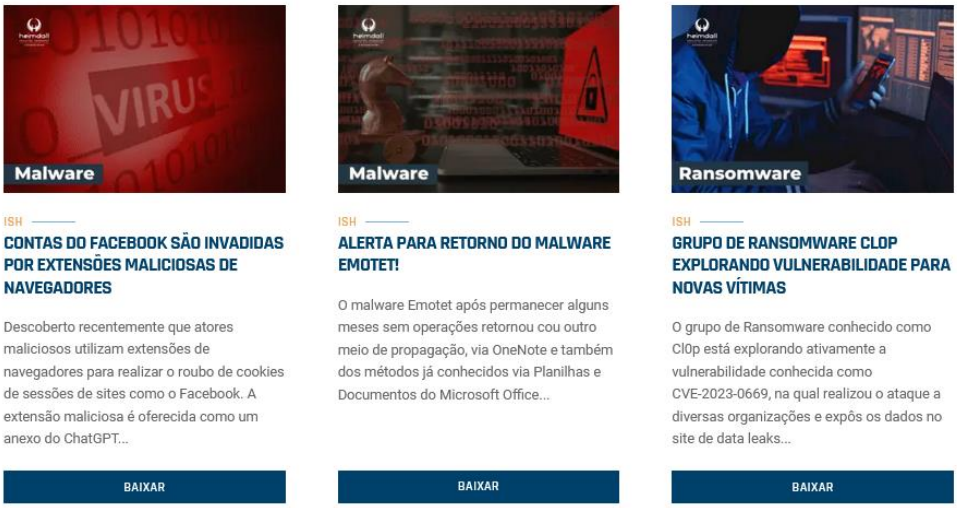
heimdall
security research
A DIVISION OF ISH

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 TABELAS

# 1 PATCH TUESDAY OUTUBRO 2024

A Microsoft por meio do seu projeto de divulgação de toda segunda terça-feira em cada mês as principais vulnerabilidades corrigidas relacionadas a seus produtos. Dentre elas, podemos mencionar a publicada neste mês de outubro de 2024, a qual realizou a correção de **118 vulnerabilidades** e, dentre elas **2 estão sobre explorações ativas**.

Das 118 vulnerabilidades, 3 são classificadas como críticas, 113 classificadas como importantes e 2 são classificadas como moderadas. Esta atualização do Patch Tuesday não incluiu as 25 falhas adicionais que a Microsoft teria abordado em seu navegador Edge baseado em Chromium no mês passado (setembro).

Das 5 das vulnerabilidades listadas como importantes e moderadas, duas delas estão sobre a exploração ativa como zero day, sendo:

| | |
|---|---|
| **CVE:** | CVE-2024-43572 |
| **Descrição:** | Vulnerabilidade de Execução Remota de Código do Console de Gerenciamento Microsoft. |
| **Pontuação:** | 7.8 Alto |
| **Exploração Detectada?** | Sim |

*Tabela 1 – CVE-2024-43572.*

| | |
|---|---|
| **CVE:** | CVE-2024-43573 |
| **Descrição:** | Vulnerabilidade de falsificação da plataforma MSHTML do Windows. |
| **Pontuação:** | 6.5 Médio |
| **Exploração Detectada?** | Sim |

*Tabela 2 – CVE-2024-43573.*

| | |
|---|---|
| **CVE:** | CVE-2024-43583 |
| **Descrição:** | Vulnerabilidade de elevação de privilégios no Winlogon. |
| **Pontuação:** | 7.8 Alto |
| **Exploração Detectada?** | Não |

*Tabela 3 – CVE-2024-43583.*

| | |
|---|---|
| **CVE:** | CVE-2024-20659 |

| | |
|---|---|
| **Descrição:** | Vulnerabilidade de desvio de recurso de segurança no Windows Hyper-V. |
| **Pontuação:** | 7.1 Alta |
| **Exploração Detectada?** | Não |

*Tabela 4 – CVE-2024-20659.*

| | |
|---|---|
| **CVE:** | CVE-2024-6197 |
| **Descrição:** | O analisador ASN1 da libcurl tem esta função utf8asn1str() usada para analisar uma string ASN.1 UTF-8. Ele pode detectar um campo inválido e retornar um erro. Infelizmente, ao fazer isso ele também invoca `free()` em um buffer localstack de 4 bytes. A maioria das implementações modernas de malloc detectam esse erro e abortam imediatamente. Alguns, entretanto, aceitam o ponteiro de entrada e adicionam essa memória à sua lista de blocos disponíveis. Isso leva à substituição da memória da pilha próxima. O conteúdo da substituição é decidido pela implementação `free()`; provavelmente serão ponteiros de memória e um conjunto de sinalizadores. O resultado mais provável da exploração desta falha é um acidente, embora não se possa excluir que resultados mais sérios possam ser obtidos em circunstâncias especiais. |
| **Pontuação:** | 7.5 Alta |
| **Exploração Detectada?** | Não |

*Tabela 5 – CVE-2024-6197.*

A vulnerabilidade **CVE-2024-43573** é semelhante a outras duas vulnerabilidades (**CVE-2024-38112 e CVE-2024-43461**) identificadas como exploradas antes de julho de 2024 pelo ator de ameaça **Void Banshee** para realizar a entrega do malware **Atlantida Stealer**.

De acordo com a declaração da Microsoft, esta não afirmou como as vulnerabilidades estavam sendo exploradas por atores de ameaças. A CISA também adicionou as **CVE-2024-43572** e **CVE-2024-43573** como exploradas por atores de ameaças em 08 de outubro.

Dentre as vulnerabilidades informadas, a CVE-2024-43468, de pontuação 9.8 é mais crítica, haja vista que esta vulnerabilidade poderia permitir que atores não autenticados executassem comandos arbitrários.

## 2 LISTA DAS CVES

| Marca | CVE | Pontuação de base | Vetor CVSS | Exploração | Perguntas frequentes? | Soluções alternativas? | Mitigações? |
|---|---|---|---|---|---|---|---|
| Função: Windows Hyper-V | CVE-2024-20659 | 7,1 | CVSS:3.1/AV:A/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C | Probabilidade Menor de Exploração | **Sim** | Não | Não |
| Windows Hyper-V | CVE-2024-30092 | 8,0 | CVSS:3.1/AV:A/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | **Sim** | Não | Não |
| Partição Windows EFI | CVE-2024-37976 | 6,7 | CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | **Sim** | Não | Não |
| Windows Kernel | CVE-2024-37979 | 6,7 | CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | **Sim** | Não | Não |
| Partição Windows EFI | CVE-2024-37982 | 6,7 | CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | **Sim** | Não | Não |
| Partição Windows EFI | CVE-2024-37983 | 6,7 | CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | **Sim** | Não | Não |
| OpenSSH para Windows | CVE-2024-38029 | 7,5 | CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | **Sim** | Não | Não |
| Monitor do Azure | CVE-2024-38097 | 7,1 | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:H/E:U/RL:O/RC:C | Exploração Improvável | **Sim** | Não | Não |
| Windows Netlogon | CVE-2024-38124 | 9,0 | CVSS:3.1/AV:A/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | **Sim** | Não | **Sim** |
| Windows Kerberos | CVE-2024-38129 | 7,5 | CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | **Sim** | Não | Não |
| BranchCache | CVE-2024-38149 | 7,5 | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | Não | Não | Não |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Azure Stack | CVE-2024-38179 | 8,8 | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | Não | Não | Não |
| Windows RRAS (Serviço de Roteamento e Acesso Remoto) | CVE-2024-38212 | 8,8 | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | **Sim** | Não | Não |
| .NET e Visual Studio | CVE-2024-38229 | 8,1 | CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | **Sim** | Não | Não |
| Windows RRAS (Serviço de Roteamento e Acesso Remoto) | CVE-2024-38261 | 7,8 | CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | **Sim** | Não | Não |
| Serviço de Licenciamento da Área de Trabalho Remota do Windows | CVE-2024-38262 | 7,5 | CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | **Sim** | Não | Não |
| Windows RRAS (Serviço de Roteamento e Acesso Remoto) | CVE-2024-38265 | 8,8 | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | **Sim** | Não | Não |
| Windows RRAS (Serviço de Roteamento e Acesso Remoto) | CVE-2024-43453 | 8,8 | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | **Sim** | Não | Não |
| Serviços de Área de Trabalho Remota do Windows | CVE-2024-43456 | 4,8 | CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | **Sim** | Não | Não |
| Microsoft Configuration Manager | CVE-2024-43468 | 9,8 | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | **Sim** | **Sim** | Não |
| Service Fabric | CVE-2024-43480 | 6,6 | CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | **Sim** | Não | Não |
| Power BI | CVE-2024-43481 | 6,5 | CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | **Sim** | Não | Não |
| .NET, .NET Framework, Visual Studio | CVE-2024-43483 | 7,5 | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | Não | Não | Não |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| .NET, .NET Framework, Visual Studio | CVE-2024-43484 | 7,5 | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | Não | Não | Não |
| .NET e Visual Studio | CVE-2024-43485 | 7,5 | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | Não | Não | Não |
| Visual Studio Code | CVE-2024-43488 | 8,8 | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | **Sim** | Não | Não |
| DeepSpeed | CVE-2024-43497 | 8,4 | CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | **Sim** | Não | Não |
| ReFS (Sistema de Arquivos Resiliente) do Windows | CVE-2024-43500 | 5,5 | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | **Sim** | Não | Não |
| Driver do Sistema de Arquivos de Log Comum do Windows | CVE-2024-43501 | 7,8 | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | **Sim** | Não | Não |
| Windows Kernel | CVE-2024-43502 | 7,1 | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:H/E:U/RL:O/RC:C | Probabilidade Maior de Exploração | **Sim** | Não | Não |
| Microsoft Office SharePoint | CVE-2024-43503 | 7,8 | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | **Sim** | Não | Não |
| Microsoft Office Excel | CVE-2024-43504 | 7,8 | CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | **Sim** | Não | Não |
| Microsoft Office Visio | CVE-2024-43505 | 7,8 | CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | **Sim** | Não | Não |
| BranchCache | CVE-2024-43506 | 7,5 | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | Não | Não | Não |
| Componente Microsoft Graphics | CVE-2024-43508 | 5,5 | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | **Sim** | Não | Não |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Componente Microsoft Graphics | CVE-2024-43509 | 7,8 | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C | Probabilidade Maior de Exploração | **Sim** | Não | Não |
| Windows Kernel | CVE-2024-43511 | 7,0 | CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | **Sim** | Não | Não |
| Serviço de Gerenciamento de Armazenamento com Base em Padrões do Windows | CVE-2024-43512 | 6,5 | CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | Não | Não | Não |
| Windows BitLocker | CVE-2024-43513 | 6,4 | CVSS:3.1/AV:P/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | **Sim** | Não | Não |
| Windows NTFS | CVE-2024-43514 | 7,8 | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | **Sim** | Não | Não |
| iSCSI (Interface de sistemas de computadores pequenos da Internet) | CVE-2024-43515 | 7,5 | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | Não | Não | Não |
| Modo de Kernel Seguro do Windows | CVE-2024-43516 | 7,8 | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | **Sim** | Não | Não |
| Microsoft ActiveX | CVE-2024-43517 | 8,8 | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | **Sim** | Não | Não |
| Servidor de Telefonia do Windows | CVE-2024-43518 | 8,8 | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | **Sim** | Não | Não |
| Provedor Microsoft WDAC OLE DB para SQL | CVE-2024-43519 | 8,8 | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | **Sim** | Não | Não |
| Windows Kernel | CVE-2024-43520 | 5,0 | CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | **Sim** | Não | Não |
| Função: Windows Hyper-V | CVE-2024-43521 | 7,5 | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | Não | Não | Não |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| LSA (Autoridade de Segurança Local) do Windows | CVE-2024-43522 | 7,0 | CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | **Sim** | Não | Não |
| Banda larga móvel do Windows | CVE-2024-43523 | 6,8 | CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | **Sim** | Não | Não |
| Banda larga móvel do Windows | CVE-2024-43524 | 6,8 | CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | **Sim** | Não | Não |
| Banda larga móvel do Windows | CVE-2024-43525 | 6,8 | CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | **Sim** | Não | Não |
| Banda larga móvel do Windows | CVE-2024-43526 | 6,8 | CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | **Sim** | Não | Não |
| Windows Kernel | CVE-2024-43527 | 7,8 | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | **Sim** | Não | Não |
| Modo de Kernel Seguro do Windows | CVE-2024-43528 | 7,8 | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | **Sim** | Não | Não |
| Componentes do Spooler de Impressão do Windows | CVE-2024-43529 | 7,3 | CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | **Sim** | Não | Não |
| Mapeador de Ponto de Extremidade RPC | CVE-2024-43532 | 8,8 | CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | **Sim** | Não | Não |
| Cliente da Área de Trabalho Remota | CVE-2024-43533 | 8,8 | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | **Sim** | Não | **Sim** |
| Componente Microsoft Graphics | CVE-2024-43534 | 6,5 | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | **Sim** | Não | Não |
| Drivers de Modo Kernel do Windows | CVE-2024-43535 | 7,0 | CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | **Sim** | Não | Não |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Banda larga móvel do Windows | CVE-2024-43536 | 6,8 | CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | **Sim** | Não | Não |
| Banda larga móvel do Windows | CVE-2024-43537 | 6,5 | CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | **Sim** | Não | Não |
| Banda larga móvel do Windows | CVE-2024-43538 | 6,5 | CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | **Sim** | Não | Não |
| Banda larga móvel do Windows | CVE-2024-43540 | 6,5 | CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | **Sim** | Não | Não |
| Protocolo de registro de certificado simples da Microsoft | CVE-2024-43541 | 7,5 | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | Não | Não | Não |
| Banda larga móvel do Windows | CVE-2024-43542 | 6,5 | CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | **Sim** | Não | Não |
| Banda larga móvel do Windows | CVE-2024-43543 | 6,8 | CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | **Sim** | Não | Não |
| Protocolo de registro de certificado simples da Microsoft | CVE-2024-43544 | 7,5 | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | Não | Não | Não |
| OCSP (Protocolo de Status de Certificado Online) do Windows | CVE-2024-43545 | 7,5 | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | Não | Não | Não |
| Serviços de Criptografia do Windows | CVE-2024-43546 | 5,6 | CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:N/A:N/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | **Sim** | Não | Não |
| Windows Kerberos | CVE-2024-43547 | 6,5 | CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | **Sim** | Não | Não |
| Windows RRAS (Serviço de Roteamento e Acesso Remoto) | CVE-2024-43549 | 8,8 | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | **Sim** | Não | Não |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Canal de Segurança do Windows | CVE-2024-43550 | 7,4 | CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | **Sim** | Não | Não |
| Armazenamento do Windows | CVE-2024-43551 | 7,8 | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | **Sim** | Não | Não |
| Shell do Windows | CVE-2024-43552 | 7,3 | CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | **Sim** | Não | Não |
| Windows NT OS Kernel | CVE-2024-43553 | 7,4 | CVSS:3.1/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | **Sim** | Não | Não |
| Drivers de Modo Kernel do Windows | CVE-2024-43554 | 5,5 | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | **Sim** | Não | Não |
| Banda larga móvel do Windows | CVE-2024-43555 | 6,5 | CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | **Sim** | Não | Não |
| Componente Microsoft Graphics | CVE-2024-43556 | 7,8 | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C | Probabilidade Maior de Exploração | **Sim** | Não | Não |
| Banda larga móvel do Windows | CVE-2024-43557 | 6,5 | CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | **Sim** | Não | Não |
| Banda larga móvel do Windows | CVE-2024-43558 | 6,5 | CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | **Sim** | Não | Não |
| Banda larga móvel do Windows | CVE-2024-43559 | 6,5 | CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | **Sim** | Não | Não |
| Driver de porta de armazenamento do Windows | CVE-2024-43560 | 7,8 | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C | Probabilidade Maior de Exploração | **Sim** | Não | Não |
| Banda larga móvel do Windows | CVE-2024-43561 | 6,5 | CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | **Sim** | Não | Não |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| NAT (Conversão de Endereço de Rede) do Windows | CVE-2024-43562 | 7,5 | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | Não | Não | Não |
| Driver de Função Auxiliar do Windows para WinSock | CVE-2024-43563 | 7,8 | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | **Sim** | Não | Não |
| Windows RRAS (Serviço de Roteamento e Acesso Remoto) | CVE-2024-43564 | 8,8 | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | **Sim** | Não | Não |
| NAT (Conversão de Endereço de Rede) do Windows | CVE-2024-43565 | 7,5 | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | Não | Não | Não |
| Função: Windows Hyper-V | CVE-2024-43567 | 7,5 | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | Não | Não | Não |
| Windows Kernel | CVE-2024-43570 | 6,4 | CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | **Sim** | Não | Não |
| Sudo para Windows | CVE-2024-43571 | 5,6 | CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:L/A:N/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | **Sim** | Não | **Sim** |
| Console de Gerenciamento Microsoft | CVE-2024-43572 | 7,8 | CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C | Exploração detectada | **Sim** | Não | Não |
| Plataforma MSHTML do Windows | CVE-2024-43573 | 6,5 | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:F/RL:O/RC:C | Exploração detectada | **Sim** | Não | Não |
| Microsoft Windows Speech | CVE-2024-43574 | 8,3 | CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | **Sim** | Não | Não |
| Função: Windows Hyper-V | CVE-2024-43575 | 7,5 | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | Não | Não | Não |
| Microsoft Office | CVE-2024-43576 | 7,8 | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | **Sim** | Não | **Sim** |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| OpenSSH para Windows | CVE-2024-43581 | 7,1 | CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C | Probabilidade Maior de Exploração | **Sim** | Não | Não |
| Área de Trabalho Remota do Windows | CVE-2024-43582 | 8,1 | CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | **Sim** | Não | Não |
| Winlogon | CVE-2024-43583 | 7,8 | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C | Probabilidade Maior de Exploração | **Sim** | Não | Não |
| Scripts do Windows | CVE-2024-43584 | 7,7 | CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | **Sim** | Não | Não |
| Proteção de integridade de código | CVE-2024-43585 | 5,5 | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:N/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | **Sim** | Não | **Sim** |
| Windows RRAS (Serviço de Roteamento e Acesso Remoto) | CVE-2024-43589 | 8,8 | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RC:C | Probabilidade Menor de Exploração | Não | Não | Não |
| Instalador redistribuível do Visual C++ | CVE-2024-43590 | 7,8 | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | **Sim** | Não | Não |
| CLI do Azure | CVE-2024-43591 | 8,7 | CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:N/I:H/A:H/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | **Sim** | Não | Não |
| Windows RRAS (Serviço de Roteamento e Acesso Remoto) | CVE-2024-43592 | 8,8 | CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | **Sim** | Não | Não |
| Windows RRAS (Serviço de Roteamento e Acesso Remoto) | CVE-2024-43593 | 8,8 | CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | **Sim** | Não | Não |
| Cliente da Área de Trabalho Remota | CVE-2024-43599 | 8,8 | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | **Sim** | Não | Não |
| Visual Studio Code | CVE-2024-43601 | 7,1 | CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | **Sim** | Não | Não |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Visual Studio | CVE-2024-43603 | 5,5 | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | Não | Não | Não |
| Outlook para Android | CVE-2024-43604 | 5,7 | CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | **Sim** | Não | Não |
| Windows RRAS (Serviço de Roteamento e Acesso Remoto) | CVE-2024-43607 | 8,8 | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | **Sim** | Não | Não |
| Windows RRAS (Serviço de Roteamento e Acesso Remoto) | CVE-2024-43608 | 8,8 | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | **Sim** | Não | Não |
| Microsoft Office | CVE-2024-43609 | 6,5 | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C | Probabilidade Maior de Exploração | **Sim** | Não | **Sim** |
| Windows RRAS (Serviço de Roteamento e Acesso Remoto) | CVE-2024-43611 | 8,8 | CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | **Sim** | Não | Não |
| Power BI | CVE-2024-43612 | 6,9 | CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:H/I:L/A:N/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | **Sim** | Não | Não |
| Microsoft Defender for Endpoint | CVE-2024-43614 | 5,5 | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | Não | Não | Não |
| OpenSSH para Windows | CVE-2024-43615 | 7,1 | CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C | Probabilidade Maior de Exploração | **Sim** | Não | Não |
| Microsoft Office | CVE-2024-43616 | 7,8 | CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C | Probabilidade Menor de Exploração | **Sim** | Não | Não |

*Tabela 6 – Vulnerabilidades tratadas pela Microsoft.*

# 3 REFERÊNCIAS


- **Heimdall *by* ISH Tecnologia**
- **Release notes for Microsoft Edge Security Updates – Microsoft**
- **Atualizações de Segurança de Outubro de 2024 – Microsoft**


# 4 AUTORES


- **Caique Barqueta**

heimdall
security research
A DIVISION OF ISH