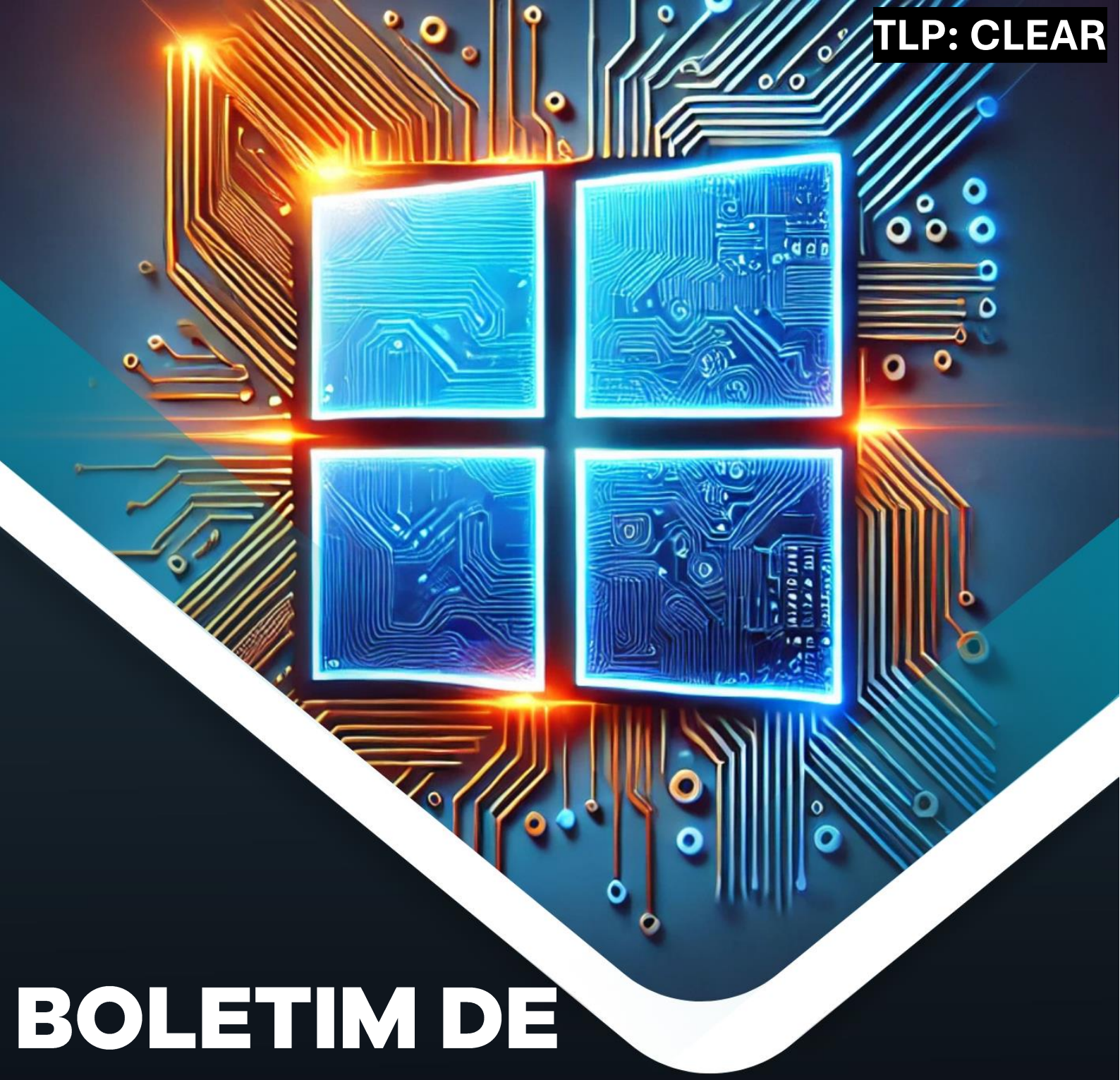
TLP: CLEAR



BOLETIM DE SEGURANÇA

Atualizações da Microsoft (Patch Tuesday) - janeiro de 2025

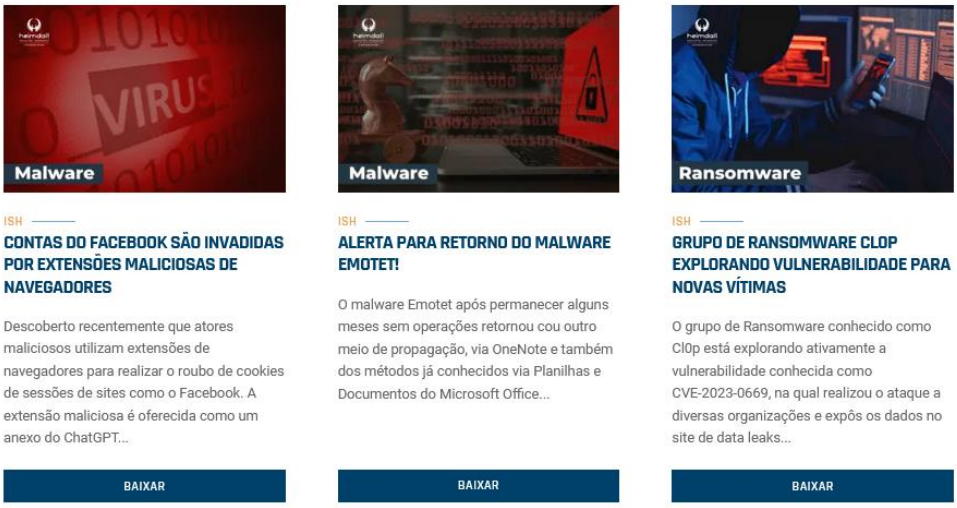
heimdall
security research
A DIVISION OF ISH

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 JANEIRO 2025

A Microsoft, por meio de seu programa mensal conhecido como Patch Tuesday, divulgado em cada mês, informa as principais vulnerabilidades corrigidas em seus produtos. Na atualização de janeiro de 2025, foram tratadas **159 vulnerabilidade** que impactam diversos serviços essenciais, como Windows, Microsoft Office, .NET Framework e outras plataformas críticas.

As vulnerabilidades foram distribuídas nas seguintes categorias:

- Elevação de Privilégio: 40
- Bypass de Funcionalidade de Segurança: 14
- Execução Remota de Código: 58
- Divulgação de Informações: 24
- Negação de Serviço: 20
- Falsificação (Spoofing): 3

Entre essas vulnerabilidades, 8 foram identificadas como zero-day, 3 delas estão sobre a exploração ativa, sendo:

CVE:	CVE-2025-21333
Descrição:	Vulnerabilidade de elevação de privilégio do VSP de integração do kernel do Windows Hyper-V NT
Pontuação:	7.8 Alto
Exploração Detectada?	Sim

Tabela 1 – CVE-2025-21333.

CVE:	CVE-2025-21334
Descrição:	Vulnerabilidade de elevação de privilégio do VSP de integração do kernel do Windows Hyper-V NT
Pontuação:	7.8 Alto
Exploração Detectada?	Sim

Tabela 2 – CVE-2025-21334.

CVE:	CVE-2025-21335

Descrição:	Vulnerabilidade de elevação de privilégio do VSP de integração do kernel do Windows Hyper-V NT
Pontuação:	7.8 Alto
Exploração Detectada?	Sim

Tabela 3 – CVE-2025-21335.

A Microsoft solucionou três falhas de elevação de privilégio no Windows Hyper-V que já estavam sendo utilizadas em ataques para obter acesso com privilégios de sistema em dispositivos Windows.

Não foram revelados detalhes sobre o método de exploração dessas vulnerabilidades, e todas foram reportadas de forma anônima. Considerando que os CVEs dessas três falhas são sequenciais e afetam o mesmo componente, há uma forte indicação de que elas foram descobertas ou exploradas dentro do mesmo contexto ou por meio de ataques relacionados.

2 LISTA DAS CVES

Marca	CVE	Pontuação de base	Vetor CVSS	Exploração	Perguntas frequentes?	Soluções alternativas?	Mitigações?
.NET	CVE-2025-21171	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
.NET e Visual Studio	CVE-2025-21172	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
.NET	CVE-2025-21173	8	CVSS:3.1/AV:N/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
.NET, .NET Framework, Visual Studio	CVE-2025-21176	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	CVE-2025-21178	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 Access	CVE-2025-21186	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
Power Automate	CVE-2025-21187	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
MapUrlToZone do Windows	CVE-2025-21189	4,3	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Probabilidade Maior de Exploração	**Sim**	Não	Não
Serviços de Federação do Active Directory	CVE-2025-21193	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
Agente de Ambiente de Recuperação do Windows	CVE-2025-21202	6,1	CVSS:3.1/AV:P/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
Serviço de Plataforma de Dispositivos Conectados do	CVE-2025-21207	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	**Sim**	Não	Não
Módulo de Plataforma Virtual Confiável do	CVE-2025-21210	4,2	CVSS:3.1/AV:P/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Probabilidade Maior de Exploração	**Sim**	Não	Não

Carregador de inicialização do Windows	CVE-2025-21211	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 BitLocker	CVE-2025-21213	4,6	CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Probabilidade Menor de Exploração	**Sim**	Não	Não
Windows BitLocker	CVE-2025-21214	4,2	CVSS:3.1/AV:P/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Probabilidade Menor de Exploração	**Sim**	Não	Não
Gerenciador de inicialização do Windows	CVE-2025-21215	4,6	CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Probabilidade Menor de Exploração	**Sim**	Não	Não
MOTW (Marca da Web do Windows)	CVE-2025-21217	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
Windows Kerberos	CVE-2025-21218	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	**Sim**	Não	Não
MapUrlToZone do Windows	CVE-2025-21219	4,3	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:U/RL:O/RC:C	Probabilidade Maior de Exploração	**Sim**	Não	Não
Enfileiramento de Mensagens do Windows	CVE-2025-21220	7,5	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Probabilidade Menor de Exploração	**Sim**	Não	Não
Serviço de telefonia do Windows	CVE-2025-21223	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
Serviço LPD (Daemon de Impressora de Linha)	CVE-2025-21224	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	**Sim**
Serviços de Área de Trabalho Remota do	CVE-2025-21225	5,9	CVSS:3.1/AV:N/AC:H/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
Mídia Digital do Windows	CVE-2025-21226	6,6	CVSS:3.1/AV:P/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
Mídia Digital do Windows	CVE-2025-21227	6,6	CVSS:3.1/AV:P/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

Mídia Digital do Windows	CVE-2025-21228	6,6	CVSS:3.1/AV:P/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
Mídia Digital do Windows	CVE-2025-21229	6,6	CVSS:3.1/AV:P/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
Enfileiramento de Mensagens do Windows	CVE-2025-21230	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	**Sim**	Não	Não
Auxiliar de IP	CVE-2025-21231	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	**Sim**	Não	Não
Mídia Digital do Windows	CVE-2025-21232	6,6	CVSS:3.1/AV:P/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
Serviço de telefonia do Windows	CVE-2025-21233	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 PrintWorkflowUserSvc	CVE-2025-21234	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 PrintWorkflowUserSvc	CVE-2025-21235	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
Serviço de telefonia do Windows	CVE-2025-21236	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
Serviço de telefonia do Windows	CVE-2025-21237	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
Serviço de telefonia do Windows	CVE-2025-21238	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
Serviço de telefonia do Windows	CVE-2025-21239	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
Serviço de telefonia do Windows	CVE-2025-21240	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

Serviço de telefonia do Windows	CVE-2025-21241	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 Kerberos	CVE-2025-21242	5,9	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Probabilidade Menor de Exploração	**Sim**	Não	Não
Serviço de telefonia do Windows	CVE-2025-21243	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
Serviço de telefonia do Windows	CVE-2025-21244	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
Serviço de telefonia do Windows	CVE-2025-21245	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
Serviço de telefonia do Windows	CVE-2025-21246	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
Serviço de telefonia do Windows	CVE-2025-21248	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
Mídia Digital do Windows	CVE-2025-21249	6,6	CVSS:3.1/AV:P/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
Serviço de telefonia do Windows	CVE-2025-21250	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
Enfileiramento de Mensagens do Windows	CVE-2025-21251	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	**Sim**	Não	Não
Serviço de telefonia do Windows	CVE-2025-21252	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
Mídia Digital do Windows	CVE-2025-21255	6,6	CVSS:3.1/AV:P/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
Mídia Digital do Windows	CVE-2025-21256	6,6	CVSS:3.1/AV:P/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

Serviço de Configuração Automática de WLAN do	CVE-2025-21257	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
Mídia Digital do Windows	CVE-2025-21258	6,6	CVSS:3.1/AV:P/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
Mídia Digital do Windows	CVE-2025-21260	6,6	CVSS:3.1/AV:P/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
Mídia Digital do Windows	CVE-2025-21261	6,6	CVSS:3.1/AV:P/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
Mídia Digital do Windows	CVE-2025-21263	6,6	CVSS:3.1/AV:P/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
Mídia Digital do Windows	CVE-2025-21265	6,6	CVSS:3.1/AV:P/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
Serviço de telefonia do Windows	CVE-2025-21266	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
MapUrlToZone do Windows	CVE-2025-21268	4,3	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	Probabilidade Maior de Exploração	**Sim**	Não	Não
MapUrlToZone do Windows	CVE-2025-21269	4,3	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:U/RL:O/RC:C	Probabilidade Maior de Exploração	**Sim**	Não	Não
Enfileiramento de Mensagens do Windows	CVE-2025-21270	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	**Sim**	Não	Não
Driver de Minifiltro de Arquivos de Nuvem do	CVE-2025-21271	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 COM	CVE-2025-21272	6,5	CVSS:3.1/AV:L/AC:L/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
Serviço de telefonia do Windows	CVE-2025-21273	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

Rastreamento de Eventos do Windows	CVE-2025-21274	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	**Sim**	Não	Não
Windows Installer	CVE-2025-21275	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
MapUrlToZone do Windows	CVE-2025-21276	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	**Sim**	Não	Não
Enfileiramento de Mensagens do Windows	CVE-2025-21277	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	**Sim**	Não	Não
Serviços de Área de Trabalho Remota do	CVE-2025-21278	6,2	CVSS:3.1/AV:L/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
Módulo de Plataforma Virtual Confiável do	CVE-2025-21280	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	**Sim**	Não	Não
Windows COM	CVE-2025-21281	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
Serviço de telefonia do Windows	CVE-2025-21282	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
Módulo de Plataforma Virtual Confiável do	CVE-2025-21284	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	**Sim**	Não	Não
Enfileiramento de Mensagens do Windows	CVE-2025-21285	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	**Sim**	Não	Não
Serviço de telefonia do Windows	CVE-2025-21286	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 Installer	CVE-2025-21287	7,8	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C	Probabilidade Menor de Exploração	**Sim**	Não	Não
Windows COM	CVE-2025-21288	6,5	CVSS:3.1/AV:L/AC:L/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

Enfileiramento de Mensagens do Windows	CVE-2025-21289	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	**Sim**	Não	Não
Enfileiramento de Mensagens do Windows	CVE-2025-21290	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	**Sim**	Não	Não
Windows Direct Show	CVE-2025-21291	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
Componente de Pesquisa do Microsoft Windows	CVE-2025-21292	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 Maior de Exploração	**Sim**	Não	Não
Serviços de Domínio do Active Directory	CVE-2025-21293	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
Autenticação do Microsoft Digest	CVE-2025-21294	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
Negociação Estendida do Windows SPNEGO	CVE-2025-21295	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
BranchCache	CVE-2025-21296	7,5	CVSS:3.1/AV:A/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
Serviços de Área de Trabalho Remota do	CVE-2025-21297	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 OLE	CVE-2025-21298	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 Maior de Exploração	**Sim**	**Sim**	Não
Windows Kerberos	CVE-2025-21299	7,1	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N/E:U/RL:O/RC:C	Probabilidade Maior de Exploração	**Sim**	Não	Não
Host de Dispositivo UPnP do Windows	CVE-2025-21300	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
Serviço de Geolocalização do Windows	CVE-2025-21301	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

Serviço de telefonia do Windows	CVE-2025-21302	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
Serviço de telefonia do Windows	CVE-2025-21303	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
Biblioteca Principal do Windows DWM	CVE-2025-21304	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
Serviço de telefonia do Windows	CVE-2025-21305	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
Serviço de telefonia do Windows	CVE-2025-21306	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
RMCAST (Reliable Multicast Transport	CVE-2025-21307	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**	Não	**Sim**
Temas do Windows	CVE-2025-21308	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	**Sim**
Serviços de Área de Trabalho Remota do	CVE-2025-21309	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 Maior de Exploração	**Sim**	Não	Não
Mídia Digital do Windows	CVE-2025-21310	6,6	CVSS:3.1/AV:P/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 NTLM	CVE-2025-21311	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**	Não	Não
Cartão Inteligente do Windows	CVE-2025-21312	2,4	CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:U/RL:O/RC:C	Probabilidade Menor de Exploração	**Sim**	Não	Não
Gerenciador de Contas de Segurança do Windows	CVE-2025-21313	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	**Sim**	Não	Não
Windows SmartScreen	CVE-2025-21314	6,5	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N/E:U/RL:O/RC:C	Probabilidade Maior de Exploração	**Sim**	Não	Não

Sistema de Intermediação de Arquivos da Microsoft	CVE-2025-21315	7,8	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:U/RL:O/RC:C	Probabilidade Maior de Exploração	**Sim**	Não	Não
Memória kernel do WIndows	CVE-2025-21316	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
Memória kernel do WIndows	CVE-2025-21317	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
Memória kernel do WIndows	CVE-2025-21318	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
Memória kernel do WIndows	CVE-2025-21319	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
Memória kernel do WIndows	CVE-2025-21320	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
Memória kernel do WIndows	CVE-2025-21321	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
Memória kernel do WIndows	CVE-2025-21323	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
Mídia Digital do Windows	CVE-2025-21324	6,6	CVSS:3.1/AV:P/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
Internet Explorer	CVE-2025-21326	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
Mídia Digital do Windows	CVE-2025-21327	6,6	CVSS:3.1/AV:P/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
MapUrlToZone do Windows	CVE-2025-21328	4,3	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:U/RL:O/RC:C	Probabilidade Maior de Exploração	**Sim**	Não	Não
MapUrlToZone do Windows	CVE-2025-21329	4,3	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:U/RL:O/RC:C	Probabilidade Maior de Exploração	**Sim**	Não	Não

Serviços de Área de Trabalho Remota do	CVE-2025-21330	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	**Sim**	Não	Não
Windows Installer	CVE-2025-21331	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
MapUrlToZone do Windows	CVE-2025-21332	4,3	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:U/RL:O/RC:C	Probabilidade Menor de Exploração	Não	Não	Não
Windows Hyper-V NT Kernel Integration VSP	CVE-2025-21333	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	Exploração detectada	**Sim**	Não	Não
Windows Hyper-V NT Kernel Integration VSP	CVE-2025-21334	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	Exploração detectada	**Sim**	Não	Não
Windows Hyper-V NT Kernel Integration VSP	CVE-2025-21335	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	Exploração detectada	**Sim**	Não	Não
Serviços de Criptografia do Windows	CVE-2025-21336	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 Win32K - GRFX	CVE-2025-21338	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
Serviço de telefonia do Windows	CVE-2025-21339	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 Hello	CVE-2025-21340	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
Mídia Digital do Windows	CVE-2025-21341	6,6	CVSS:3.1/AV:P/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
Serviço de usuário de defesa contra ameaças da	CVE-2025-21343	7,5	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C	Probabilidade Menor de Exploração	**Sim**	Não	Não
Microsoft Office SharePoint	CVE-2025-21344	7,8	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RC:C	Probabilidade Menor de Exploração	**Sim**	Não	Não

Microsoft Office Visio	CVE-2025-21345	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	CVE-2025-21346	7,1	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:H/E:U/RL:O/RC:C	Probabilidade Menor de Exploração	**Sim**	Não	Não
Microsoft Office SharePoint	CVE-2025-21348	7,2	CVSS:3.1/AV:N/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
Microsoft Office Excel	CVE-2025-21354	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 Maior de Exploração	**Sim**	Não	Não
Microsoft Office Visio	CVE-2025-21356	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 Outlook	CVE-2025-21357	6,7	CVSS:3.1/AV:L/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
MAU (Microsoft AutoUpdate)	CVE-2025-21360	7,8	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RC:C	Probabilidade Menor de Exploração	**Sim**	Não	Não
Microsoft Office Outlook para Mac	CVE-2025-21361	7,8	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RC:C	Probabilidade Menor de Exploração	**Sim**	Não	Não
Microsoft Office Excel	CVE-2025-21362	7,8	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RC:C	Probabilidade Maior de Exploração	**Sim**	Não	Não
Microsoft Office Word	CVE-2025-21363	7,8	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RC:C	Probabilidade Menor de Exploração	**Sim**	Não	Não
Microsoft Office Excel	CVE-2025-21364	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 Maior de Exploração	**Sim**	Não	Não
Microsoft Office	CVE-2025-21365	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 Maior de Exploração	**Sim**	Não	Não
Microsoft Office Access	CVE-2025-21366	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

Enclave de VBS (Segurança baseada em virtualização)	CVE-2025-21370	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
Sistema de Intermediação de Arquivos da Microsoft	CVE-2025-21372	7,8	CVSS:3.1/AV:L/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
Serviço CSC (Cache do lado do cliente) do Windows	CVE-2025-21374	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
Serviço CSC (Cache do lado do cliente) do Windows	CVE-2025-21378	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
Recursos de SaaS do Azure Marketplace	CVE-2025-21380	8,8	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	N/A	**Sim**	Não	Não
Componente Microsoft Graphics	CVE-2025-21382	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 Purview	CVE-2025-21385	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	N/A	**Sim**	Não	Não
Host de Dispositivo UPnP do Windows	CVE-2025-21389	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 SharePoint	CVE-2025-21393	6,3	CVSS:3.1/AV:N/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	Não
Microsoft Office Access	CVE-2025-21395	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 OneNote	CVE-2025-21402	7,8	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RC:C	Probabilidade Menor de Exploração	**Sim**	Não	Não
Gerente de gateway do Microsoft Azure	CVE-2025-21403	6,4	CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:N/E:U/RC:C	Probabilidade Menor de Exploração	**Sim**	Não	Não
Visual Studio	CVE-2025-21405	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	Não	Não	Não

Serviço de telefonia do Windows	CVE-2025-21409	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
Serviço de telefonia do Windows	CVE-2025-21411	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
Serviço de telefonia do Windows	CVE-2025-21413	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
Serviço de telefonia do Windows	CVE-2025-21417	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

Tabela 4 – Vulnerabilidades tratadas pela Microsoft.

3 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Release notes for Microsoft Edge Security Updates – Microsoft**
- **Atualizações de Segurança de Janeiro de 2025 – Microsoft**
- **Bleeping Computer**

4 AUTORES

- **Rafael Salomé**

heimdall
security research
A DIVISION OF ISH