ALERTA DE VULNERABILIDADE

Patch Tuesday de Maio de 2024

heimdall
security research
A DIVISION OF ISH

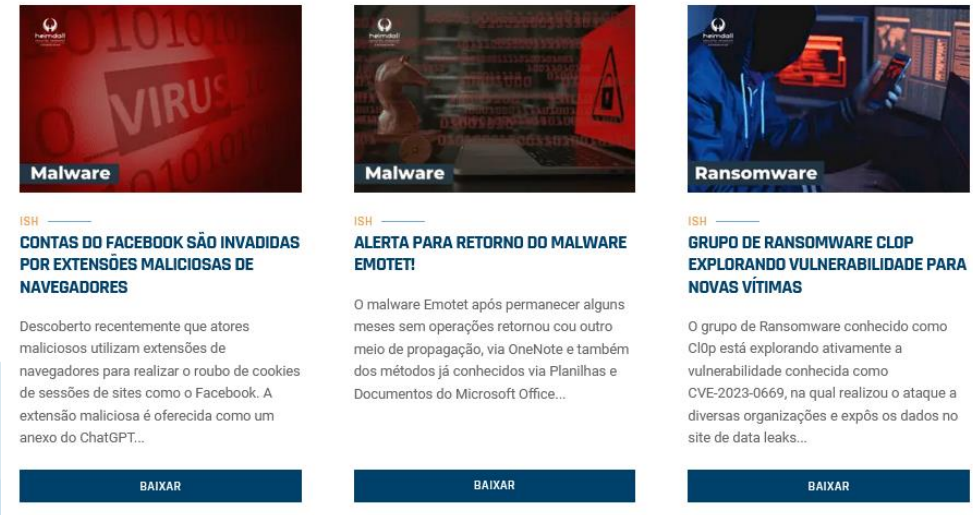
TLP: CLEAR

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



Sumário

LISTA DE TABELAS

1 SUMÁRIO EXECUTIVO

Na terça feira saiu o Patch Tuesday de maio de 2024 da Microsoft, o qual incluiu atualizações de segurança para um total de 61 falhas e 03 zero days que estavam sendo explorados ativamente.

Abaixo segue os bugs classificados por categoria de vulnerabilidade:

- 17 Vulnerabilidades de elevação de privilégio
- 2 Vulnerabilidades de desvio de recursos de segurança
- 27 Vulnerabilidades de execução remota de código
- 7 Vulnerabilidades de divulgação de informações
- 3 Vulnerabilidades de negação de serviço
- 4 vulnerabilidades de falsificação

Um total de 61 falhas foram identificadas, excluindo-se as 2 que foram solucionadas no Microsoft Edge em 2 de maio, além de mais 4 que foram corrigidas em 10 de maio.

2 ZERO DAYS EXPLORADOS EM ATAQUES

Neste mês, durante o Patch Tuesday, foram resolvidas duas vulnerabilidades de *zero day* que estavam sendo exploradas por malwares em ataques em andamento e uma divulgada publicamente.

Segue um resumo das vulnerabilidades *zero days* abordadas e suas explorações por atores maliciosos:

CVE-2024-30040 - Vulnerabilidade de desvio de recurso de segurança da plataforma Windows MSHTML

Foi implementado correções para este desvio ativamente explorado que afetava as proteções OLE no Microsoft 365 e no Microsoft Office, visando proteger os usuários contra vulnerabilidades em controles COM/OLE. Segundo a Microsoft, um atacante precisaria persuadir o usuário a carregar um arquivo malicioso em um sistema vulnerável, geralmente através de iscas em e-mails ou mensagens instantâneas. Posteriormente, o usuário teria que manipular o arquivo especialmente criado, sem necessariamente clicar ou abrir o arquivo malicioso.

Além disso, a Microsoft alertou que um invasor não autenticado que explorasse com sucesso essa vulnerabilidade poderia executar código arbitrário no contexto do usuário ao persuadir o usuário a abrir um documento malicioso. A origem dos ataques que exploraram essa falha e quem a descobriu ainda não foram identificados.

CVE-2024-30051 - Vulnerabilidade de elevação de privilégio da biblioteca principal do Windows DWM

A Microsoft identificou que esta vulnerabilidade estava sendo explorada na biblioteca principal do Windows DWM, o que pode conceder privilégios de SYSTEM. A Kaspersky observou que os ataques recentes de phishing do malware Qakbot tiraram proveito disso, usando documentos maliciosos para alcançar tal acesso em dispositivos Windows. A Microsoft também mencionou que o CVE-2024-30051 foi divulgado publicamente, embora o local exato não esteja claro, e que uma falha de negação de serviço no Microsoft Visual Studio, rastreada como CVE-2024-30046, também foi tornada pública.

3 ATUALIZAÇÕES DE SEGURANÇA DO PATCH TUESDAY

Abaixo segue a relação completa das vulnerabilidades que foram corrigidas nas atualizações do Patch Tuesday de maio de 2024, disponibilizadas pela Microsoft.

Tag	CVE ID	CVE Title	Severity
.NET and Visual Studio	CVE-2024-30045	.NET and Visual Studio Remote Code Execution Vulnerability	Important
Azure Migrate	CVE-2024-30053	Azure Migrate Cross-Site Scripting Vulnerability	Important
Microsoft Bing	CVE-2024-30041	Microsoft Bing Search Spoofing Vulnerability	Important
Microsoft Brokering File System	CVE-2024-30007	Microsoft Brokering File System Elevation of Privilege Vulnerability	Important
Microsoft Dynamics 365 Customer Insights	CVE-2024-30048	Dynamics 365 Customer Insights Spoofing Vulnerability	Important
Microsoft Dynamics 365 Customer Insights	CVE-2024-30047	Dynamics 365 Customer Insights Spoofing Vulnerability	Important
Microsoft Edge (Chromium-based)	CVE-2024-4558	Chromium: CVE-2024-4558 Use after free in ANGLE	Unknown
Microsoft Edge (Chromium-based)	CVE-2024-4331	Chromium: CVE-2024-4331 Use after free in Picture In Picture	Unknown
Microsoft Edge (Chromium-based)	CVE-2024-4671	Chromium: CVE-2024-4671 Use after free in Visuals	Unknown

Microsoft Edge (Chromium-based)	CVE-2024-30055	Microsoft Edge (Chromium-based) Spoofing Vulnerability	Low
Microsoft Edge (Chromium-based)	CVE-2024-4368	Chromium: CVE-2024-4368 Use after free in Dawn	Unknown
Microsoft Edge (Chromium-based)	CVE-2024-4559	Chromium: CVE-2024-4559 Heap buffer overflow in WebAudio	Unknown
Microsoft Intune	CVE-2024-30059	Microsoft Intune for Android Mobile Application Management Tampering Vulnerability	Important
Microsoft Office Excel	CVE-2024-30042	Microsoft Excel Remote Code Execution Vulnerability	Important
Microsoft Office SharePoint	CVE-2024-30044	Microsoft SharePoint Server Remote Code Execution Vulnerability	**Critical**
Microsoft Office SharePoint	CVE-2024-30043	Microsoft SharePoint Server Information Disclosure Vulnerability	Important

Microsoft WDAC OLE DB provider for SQL	CVE-2024-30006	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability	Important
Microsoft Windows SCSI Class System File	CVE-2024-29994	Microsoft Windows SCSI Class System File Elevation of Privilege Vulnerability	Important
Microsoft Windows Search Component	CVE-2024-30033	Windows Search Service Elevation of Privilege Vulnerability	Important
Power BI	CVE-2024-30054	Microsoft Power BI Client JavaScript SDK Information Disclosure Vulnerability	Important
Visual Studio	CVE-2024-30046	Visual Studio Denial of Service Vulnerability	Important
Visual Studio	CVE-2024-32004	GitHub: CVE-2024-32004 Remote Code Execution while cloning special-crafted local repositories	Important
Visual Studio	CVE-2024-32002	CVE-2024-32002 Recursive clones on case-insensitive filesystems that support symlinks are susceptible to Remote Code Execution	Important
Windows Cloud Files Mini Filter Driver	CVE-2024-30034	Windows Cloud Files Mini Filter Driver Information Disclosure Vulnerability	Important

Windows CNG Key Isolation Service	CVE-2024-30031	Windows CNG Key Isolation Service Elevation of Privilege Vulnerability	Important
Windows Common Log File System Driver	CVE-2024-29996	Windows Common Log File System Driver Elevation of Privilege Vulnerability	Important
Windows Common Log File System Driver	CVE-2024-30037	Windows Common Log File System Driver Elevation of Privilege Vulnerability	Important
Windows Common Log File System Driver	CVE-2024-30025	Windows Common Log File System Driver Elevation of Privilege Vulnerability	Important
Windows Cryptographic Services	CVE-2024-30020	Windows Cryptographic Services Remote Code Execution Vulnerability	Important
Windows Cryptographic Services	CVE-2024-30016	Windows Cryptographic Services Information Disclosure Vulnerability	Important
Windows Deployment Services	CVE-2024-30036	Windows Deployment Services Information Disclosure Vulnerability	Important
Windows DHCP Server	CVE-2024-30019	DHCP Server Service Denial of Service Vulnerability	Important
Windows DWM Core Library	CVE-2024-30008	Windows DWM Core Library Information Disclosure Vulnerability	Important
Windows DWM Core Library	CVE-2024-30051	Windows DWM Core Library Elevation of Privilege Vulnerability	Important

Windows DWM Core Library	CVE-2024-30035	Windows DWM Core Library Elevation of Privilege Vulnerability	Important
Windows DWM Core Library	CVE-2024-30032	Windows DWM Core Library Elevation of Privilege Vulnerability	Important
Windows Hyper-V	CVE-2024-30011	Windows Hyper-V Denial of Service Vulnerability	Important
Windows Hyper-V	CVE-2024-30017	Windows Hyper-V Remote Code Execution Vulnerability	Important
Windows Hyper-V	CVE-2024-30010	Windows Hyper-V Remote Code Execution Vulnerability	Important
Windows Kernel	CVE-2024-30018	Windows Kernel Elevation of Privilege Vulnerability	Important
Windows Mark of the Web (MOTW)	CVE-2024-30050	Windows Mark of the Web Security Feature Bypass Vulnerability	Moderate
Windows Mobile Broadband	CVE-2024-30002	Windows Mobile Broadband Driver Remote Code Execution Vulnerability	Important

Windows Mobile Broadband	CVE-2024-29997	Windows Mobile Broadband Driver Remote Code Execution Vulnerability	Important
Windows Mobile Broadband	CVE-2024-30003	Windows Mobile Broadband Driver Remote Code Execution Vulnerability	Important
Windows Mobile Broadband	CVE-2024-30012	Windows Mobile Broadband Driver Remote Code Execution Vulnerability	Important
Windows Mobile Broadband	CVE-2024-29999	Windows Mobile Broadband Driver Remote Code Execution Vulnerability	Important
Windows Mobile Broadband	CVE-2024-29998	Windows Mobile Broadband Driver Remote Code Execution Vulnerability	Important
Windows Mobile Broadband	CVE-2024-30000	Windows Mobile Broadband Driver Remote Code Execution Vulnerability	Important
Windows Mobile Broadband	CVE-2024-30005	Windows Mobile Broadband Driver Remote Code Execution Vulnerability	Important

Windows Mobile Broadband	CVE-2024-30004	Windows Mobile Broadband Driver Remote Code Execution Vulnerability	Important
Windows Mobile Broadband	CVE-2024-30021	Windows Mobile Broadband Driver Remote Code Execution Vulnerability	Important
Windows Mobile Broadband	CVE-2024-30001	Windows Mobile Broadband Driver Remote Code Execution Vulnerability	Important
Windows MSHTML Platform	CVE-2024-30040	Windows MSHTML Platform Security Feature Bypass Vulnerability	Important
Windows NTFS	CVE-2024-30027	NTFS Elevation of Privilege Vulnerability	Important
Windows Remote Access Connection Manager	CVE-2024-30039	Windows Remote Access Connection Manager Information Disclosure Vulnerability	Important
Windows Routing and Remote Access Service (RRAS)	CVE-2024-30009	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	Important
Windows Routing and Remote Access Service (RRAS)	CVE-2024-30024	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	Important

Windows Routing and Remote Access Service (RRAS)	CVE-2024-30015	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	Important
Windows Routing and Remote Access Service (RRAS)	CVE-2024-30029	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	Important
Windows Routing and Remote Access Service (RRAS)	CVE-2024-30023	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	Important
Windows Routing and Remote Access Service (RRAS)	CVE-2024-30014	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	Important
Windows Routing and Remote Access Service (RRAS)	CVE-2024-30022	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	Important
Windows Task Scheduler	CVE-2024-26238	Microsoft PLUGScheduler Scheduled Task Elevation of Privilege Vulnerability	Important
Windows Win32K - GRFX	CVE-2024-30030	Win32k Elevation of Privilege Vulnerability	Important
Windows Win32K - ICOMP	CVE-2024-30038	Win32k Elevation of Privilege Vulnerability	Important

Windows Win32K - ICOMP	CVE-2024-30049	Windows Win32 Kernel Subsystem Elevation of Privilege Vulnerability	Important
Windows Win32K - ICOMP	CVE-2024-30028	Win32k Elevation of Privilege Vulnerability	Important

Tabela 1 – Tabela das vulnerabilidades do Patch Tuesday.

4 CONCLUSÃO

O Patch Tuesday da Microsoft é um evento crítico para organizações de todos os tamanhos. Ele representa uma oportunidade mensal para corrigir vulnerabilidades de segurança nos produtos da Microsoft, que são amplamente utilizados em ambientes corporativos. A correção dessas vulnerabilidades é essencial para proteger os sistemas contra ataques cibernéticos. Ao ignorar as atualizações do Patch Tuesday, as organizações ficam expostas a riscos significativos, incluindo a perda de dados, violações de segurança e interrupções operacionais.

Além disso, manter os sistemas atualizados demonstra uma postura proativa de segurança cibernética, essencial para a confiança dos clientes e a conformidade regulatória.

5 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Microsoft**
- **Bleepingcomputer**
- **Kaspersky**

6 AUTORES

- **Ismael Pereira Rocha**


heimdall
security research
A DIVISION OF ISH