ALERTA DE VULNERABILIDADE

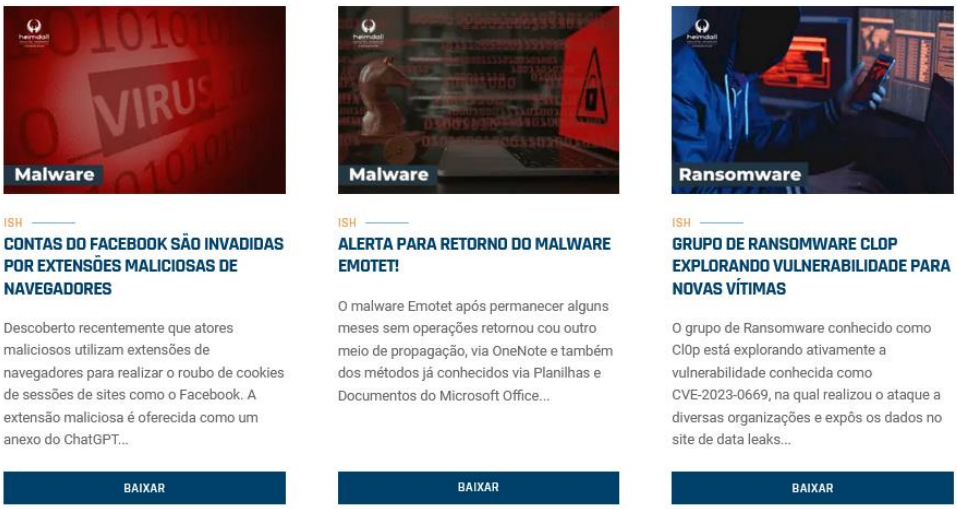
Patch Tuesday de Setembro de 2024

heimdall
security research
A DIVISION OF ISH

TLP: CLEAR

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

O Patch Tuesday de setembro de 2024 da Microsoft, incluiu atualizações de segurança para um total de 79 falhas, incluindo 03 exploradas ativamente e 01 *zero day* divulgada publicamente.

Este Patch Tuesday corrigiu 07 vulnerabilidades críticas, que eram falhas de execução remota de código ou elevação de privilégios.

Abaixo segue os bugs classificados por categoria de vulnerabilidade:

- 30 Vulnerabilidades de Elevação de Privilégios
- 4 Vulnerabilidades de desvio de recurso de segurança
- 23 Vulnerabilidades de execução remota de código
- 11 Vulnerabilidades de Divulgação de Informações
- 8 Vulnerabilidades de Negação de Serviço
- 3 Vulnerabilidades de Spoofing

2 ZEROS DAYS PUBLICADOS

Neste mês, foram corrigidas 03 vulnerabilidades que estão sendo exploradas ativamente. Uma delas foi divulgada publicamente, e outra envolve a reintrodução de CVEs antigas, sendo por isso considerada explorada.

As 03 vulnerabilidades zero-day ativamente exploradas incluídas nas atualizações são:

CVE-2024-38014 - Vulnerabilidade de elevação de privilégio do Windows Installer

Essa vulnerabilidade permite que ataques obtenham privilégios de SISTEMA em sistemas Windows. A Microsoft não compartilhou detalhes sobre como foi explorada em ataques.

CVE-2024-38217 - Vulnerabilidade de desvio do recurso de segurança do Windows Mark of the Web

Joe Desimone, da Elastic Security, divulgou publicamente uma vulnerabilidade que, segundo informações, está sendo explorada ativamente desde 2018. Desimone detalhou em seu relatório uma técnica conhecida como LNK stomping. Essa abordagem permite que arquivos LNK, criados de forma especial com caminhos de destino ou estruturas internas fora do padrão, sejam abertos sem que os avisos de segurança do Smart App Control e do Mark of the Web (MOTW) sejam acionados.

De acordo com um comunicado da Microsoft, "um invasor pode desenvolver um arquivo malicioso capaz de driblar as defesas do MOTW, o que acarretaria uma perda parcial na integridade e disponibilidade de recursos de segurança, como a verificação de reputação de aplicativos pelo SmartScreen ou o aviso de segurança legado dos Serviços de Anexos do Windows". Quando essa vulnerabilidade é explorada, o comando presente no arquivo LNK é executado sem que o usuário receba qualquer alerta..

CVE-2024-38226 - Vulnerabilidade de desvio de recurso de segurança do Microsoft Publisher

A Microsoft resolveu esta vulnerabilidade no Microsoft Publisher que permitia contornar as proteções de segurança voltadas para macros incorporadas em documentos baixados. Segundo o comunicado da Microsoft, "um invasor que conseguisse explorar essa falha com êxito poderia burlar as políticas de macro do Office, que são projetadas para bloquear arquivos considerados não confiáveis ou maliciosos".

A Microsoft também resolveu uma vulnerabilidade de zero-day que foi identificada como explorada. Essa correção foi necessária devido ao risco de reintroduzir falhas antigas que já haviam sido exploradas anteriormente, conforme descrito a seguir.

CVE-2024-43491 - Vulnerabilidade de execução remota de código do Microsoft Windows Update

A Microsoft corrigiu esta falha na pilha de serviços classificada como execução remota de código, mas que, na verdade, reintroduz uma série de vulnerabilidades previamente corrigidas em diversos programas. Segundo o comunicado da Microsoft, "estamos cientes de uma vulnerabilidade no Servicing Stack que reverteu correções para vulnerabilidades em Componentes Opcionais no Windows 10, versão 1507 (versão inicial lançada em julho de 2015)." Isso significa que sistemas rodando o Windows 10, versão 1507 (Windows 10 Enterprise 2015 LTSB e Windows 10 IoT Enterprise 2015 LTSB), que aplicaram a atualização de segurança de 12 de março de 2024 (KB5035858 - OS Build 10240.20526) ou outras atualizações até agosto de 2024, podem ser afetados. No entanto, versões posteriores do Windows 10 não são impactadas por essa vulnerabilidade.

A falha pode ser resolvida ao instalar a atualização da pilha de manutenção de setembro de 2024 (SSU KB5043936) e a atualização de segurança do Windows de setembro de 2024 (KB5043083), nesta ordem. A vulnerabilidade afeta somente o Windows 10, versão 1507, que já chegou ao fim do suporte em 2017, mas também impacta as edições Windows 10 Enterprise 2015 LTSB e Windows 10 IoT Enterprise 2015 LTSB, que ainda são suportadas. O problema é notável porque reverteu componentes opcionais, como o Active Directory Lightweight Directory Services, XPS Viewer, Internet Explorer 11, LPD Print Service, IIS e Windows Media Player para suas versões originais (RTM), reintroduzindo vulnerabilidades conhecidas e já exploradas. A Microsoft classificou essa falha como explorada porque reincorporou vulnerabilidades anteriormente ativamente exploradas. No entanto, esclareceu que a falha foi descoberta internamente e não há evidências de que seja amplamente conhecida.

3 ATUALIZAÇÕES DE SEGURANÇA DO PATCH TUESDAY

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

Tag	CVE ID	CVE Title	Severity
Azure CycleCloud	CVE-2024-43469	Azure CycleCloud Remote Code Execution Vulnerability	Important
Azure Network Watcher	CVE-2024-38188	Azure Network Watcher VM Agent Elevation of Privilege Vulnerability	Important
Azure Network Watcher	CVE-2024-43470	Azure Network Watcher VM Agent Elevation of Privilege Vulnerability	Important
Azure Stack	CVE-2024-38216	Azure Stack Hub Elevation of Privilege Vulnerability	**Critical**
Azure Stack	CVE-2024-38220	Azure Stack Hub Elevation of Privilege Vulnerability	**Critical**
Azure Web Apps	CVE-2024-38194	Azure Web Apps Elevation of Privilege Vulnerability	**Critical**
Dynamics Business Central	CVE-2024-38225	Microsoft Dynamics 365 Business Central Elevation of Privilege Vulnerability	Important
Microsoft AutoUpdate (MAU)	CVE-2024-43492	Microsoft AutoUpdate (MAU) Elevation of Privilege Vulnerability	Important
Microsoft Dynamics 365 (on-premises)	CVE-2024-43476	Microsoft Dynamics 365 (on-premises) Cross-site Scripting Vulnerability	Important

Microsoft Graphics Component	CVE-2024-38247	Windows Graphics Component Elevation of Privilege Vulnerability	Important
Microsoft Graphics Component	CVE-2024-38250	Windows Graphics Component Elevation of Privilege Vulnerability	Important
Microsoft Graphics Component	CVE-2024-38249	Windows Graphics Component Elevation of Privilege Vulnerability	Important
Microsoft Management Console	CVE-2024-38259	Microsoft Management Console Remote Code Execution Vulnerability	Important
Microsoft Office Excel	CVE-2024-43465	Microsoft Excel Elevation of Privilege Vulnerability	Important
Microsoft Office Publisher	CVE-2024-38226	Microsoft Publisher Security Feature Bypass Vulnerability	Important
Microsoft Office SharePoint	CVE-2024-38227	Microsoft SharePoint Server Remote Code Execution Vulnerability	Important

Microsoft Office SharePoint	CVE-2024-43464	Microsoft SharePoint Server Remote Code Execution Vulnerability	**Critical**
Microsoft Office SharePoint	CVE-2024-38018	Microsoft SharePoint Server Remote Code Execution Vulnerability	**Critical**
Microsoft Office SharePoint	CVE-2024-38228	Microsoft SharePoint Server Remote Code Execution Vulnerability	Important
Microsoft Office SharePoint	CVE-2024-43466	Microsoft SharePoint Server Denial of Service Vulnerability	Important
Microsoft Office Visio	CVE-2024-43463	Microsoft Office Visio Remote Code Execution Vulnerability	Important
Microsoft Outlook for iOS	CVE-2024-43482	Microsoft Outlook for iOS Information Disclosure Vulnerability	Important
Microsoft Streaming Service	CVE-2024-38245	Kernel Streaming Service Driver Elevation of Privilege Vulnerability	Important
Microsoft Streaming Service	CVE-2024-38241	Kernel Streaming Service Driver Elevation of Privilege Vulnerability	Important
Microsoft Streaming Service	CVE-2024-38242	Kernel Streaming Service Driver Elevation of Privilege Vulnerability	Important

Microsoft Streaming Service	CVE-2024-38244	Kernel Streaming Service Driver Elevation of Privilege Vulnerability	Important
Microsoft Streaming Service	CVE-2024-38243	Kernel Streaming Service Driver Elevation of Privilege Vulnerability	Important
Microsoft Streaming Service	CVE-2024-38237	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability	Important
Microsoft Streaming Service	CVE-2024-38238	Kernel Streaming Service Driver Elevation of Privilege Vulnerability	Important
Power Automate	CVE-2024-43479	Microsoft Power Automate Desktop Remote Code Execution Vulnerability	Important
Role: Windows Hyper-V	CVE-2024-38235	Windows Hyper-V Denial of Service Vulnerability	Important
SQL Server	CVE-2024-37338	Microsoft SQL Server Native Scoring Remote Code Execution Vulnerability	Important
SQL Server	CVE-2024-37980	Microsoft SQL Server Elevation of Privilege Vulnerability	Important
SQL Server	CVE-2024-26191	Microsoft SQL Server Native Scoring Remote Code Execution Vulnerability	Important

SQL Server	CVE-2024-37339	Microsoft SQL Server Native Scoring Remote Code Execution Vulnerability	Import
SQL Server	CVE-2024-37337	Microsoft SQL Server Native Scoring Information Disclosure Vulnerability	Important
SQL Server	CVE-2024-26186	Microsoft SQL Server Native Scoring Remote Code Execution Vulnerability	Important
SQL Server	CVE-2024-37342	Microsoft SQL Server Native Scoring Information Disclosure Vulnerability	Important
SQL Server	CVE-2024-43474	Microsoft SQL Server Information Disclosure Vulnerability	Important
SQL Server	CVE-2024-37335	Microsoft SQL Server Native Scoring Remote Code Execution Vulnerability	Important
SQL Server	CVE-2024-37966	Microsoft SQL Server Native Scoring Information Disclosure Vulnerability	Important
SQL Server	CVE-2024-37340	Microsoft SQL Server Native Scoring Remote Code Execution Vulnerability	Important

SQL Server	CVE-2024-37965	Microsoft SQL Server Elevation of Privilege Vulnerability	Important
SQL Server	CVE-2024-37341	Microsoft SQL Server Elevation of Privilege Vulnerability	Important
Windows Admin Center	CVE-2024-43475	Microsoft Windows Admin Center Information Disclosure Vulnerability	Important
Windows AllJoyn API	CVE-2024-38257	Microsoft AllJoyn API Information Disclosure Vulnerability	Important
Windows Authentication Methods	CVE-2024-38254	Windows Authentication Information Disclosure Vulnerability	Important
Windows DHCP Server	CVE-2024-38236	DHCP Server Service Denial of Service Vulnerability	Important
Windows Installer	CVE-2024-38014	Windows Installer Elevation of Privilege Vulnerability	Important

Windows Kerberos	CVE-2024-38239	Windows Kerberos Elevation of Privilege Vulnerability	Important
Windows Kernel-Mode Drivers	CVE-2024-38256	Windows Kernel-Mode Driver Information Disclosure Vulnerability	Important
Windows Libarchive	CVE-2024-43495	Windows libarchive Remote Code Execution Vulnerability	Important
Windows Mark of the Web (MOTW)	CVE-2024-38217	Windows Mark of the Web Security Feature Bypass Vulnerability	Important
Windows Mark of the Web (MOTW)	CVE-2024-43487	Windows Mark of the Web Security Feature Bypass Vulnerability	Moderate
Windows MSHTML Platform	CVE-2024-43461	Windows MSHTML Platform Spoofing Vulnerability	Important
Windows Network Address Translation (NAT)	CVE-2024-38119	Windows Network Address Translation (NAT) Remote Code Execution Vulnerability	**Critical**
Windows Network Virtualization	CVE-2024-38232	Windows Networking Denial of Service Vulnerability	Important

Windows Network Virtualization	CVE-2024-38233	Windows Networking Denial of Service Vulnerability	Important
Windows Network Virtualization	CVE-2024-38234	Windows Networking Denial of Service Vulnerability	Important
Windows Network Virtualization	CVE-2024-43458	Windows Networking Information Disclosure Vulnerability	Important
Windows PowerShell	CVE-2024-38046	PowerShell Elevation of Privilege Vulnerability	Important
Windows Remote Access Connection Manager	CVE-2024-38240	Windows Remote Access Connection Manager Elevation of Privilege Vulnerability	Important
Windows Remote Desktop Licensing Service	CVE-2024-38231	Windows Remote Desktop Licensing Service Denial of Service Vulnerability	Important
Windows Remote Desktop Licensing Service	CVE-2024-38258	Windows Remote Desktop Licensing Service Information Disclosure Vulnerability	Important
Windows Remote Desktop Licensing Service	CVE-2024-43467	Windows Remote Desktop Licensing Service Remote Code Execution Vulnerability	Important
Windows Remote Desktop Licensing Service	CVE-2024-43454	Windows Remote Desktop Licensing Service Remote Code Execution Vulnerability	Important

Windows Remote Desktop Licensing Service	CVE-2024-38263	Windows Remote Desktop Licensing Service Remote Code Execution Vulnerability	Important
Windows Remote Desktop Licensing Service	CVE-2024-38260	Windows Remote Desktop Licensing Service Remote Code Execution Vulnerability	Important
Windows Remote Desktop Licensing Service	CVE-2024-43455	Windows Remote Desktop Licensing Service Spoofing Vulnerability	Important
Windows Security Zone Mapping	CVE-2024-30073	Windows Security Zone Mapping Security Feature Bypass Vulnerability	Important
Windows Setup and Deployment	CVE-2024-43457	Windows Setup and Deployment Elevation of Privilege Vulnerability	Important
Windows Standards-Based Storage Management Service	CVE-2024-38230	Windows Standards-Based Storage Management Service Denial of Service Vulnerability	Important
Windows Storage	CVE-2024-38248	Windows Storage Elevation of Privilege Vulnerability	Important
Windows TCP/IP	CVE-2024-21416	Windows TCP/IP Remote Code Execution Vulnerability	Important
Windows TCP/IP	CVE-2024-38045	Windows TCP/IP Remote Code Execution Vulnerability	Important

Windows Update	CVE-2024-43491	Microsoft Windows Update Remote Code Execution Vulnerability	**Critical**
Windows Win32K - GRFX	CVE-2024-38246	Win32k Elevation of Privilege Vulnerability	Important
Windows Win32K - ICOMP	CVE-2024-38252	Windows Win32 Kernel Subsystem Elevation of Privilege Vulnerability	Important
Windows Win32K - ICOMP	CVE-2024-38253	Windows Win32 Kernel Subsystem 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**
- **NVD**

6 AUTORES

- **Ismael Pereira Rocha**


heimdall
security research
A DIVISION OF ISH