BOLETIM DE SEGURANÇA

Patch Tuesday Microsoft – Setembro 2023

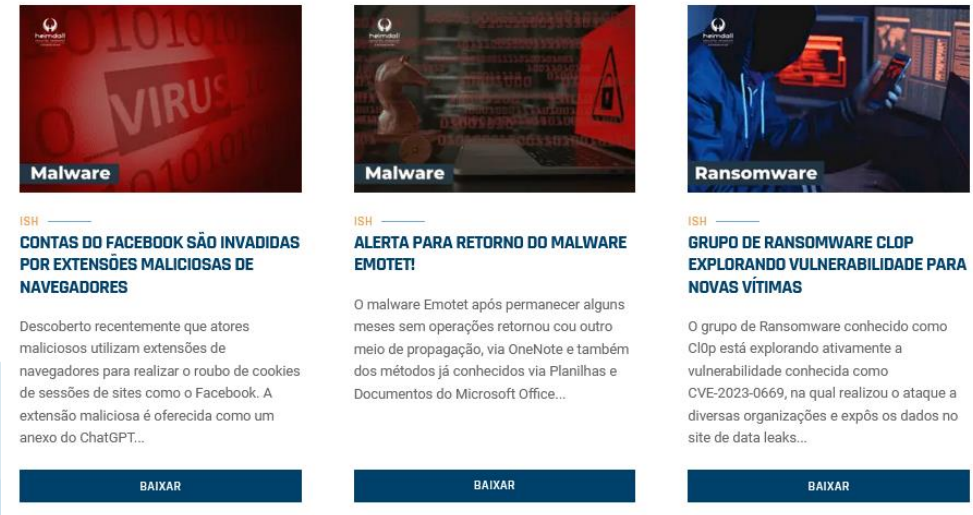
heimdall
security research
A DIVISION OF ISH

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 PATCH TUESDAY MICROSOFT

O Patch Tuesday de **setembro de 2023** da Microsoft contém atualizações para 59 falhas, incluindo duas vulnerabilidades de dia zero (zero day) exploradas ativamente.

Embora haja vinte e quatro bugs RCE corrigidos pela Microsoft, esta classificou apenas cinco como "Críticos", quatro falhas de execução remota de código e vulnerabilidade de elevação e privilégio do Serviço Azure Kubernetes.

O número de bugs em cada categoria da vulnerabilidade está listado abaixo:

- 3 vulnerabilidades de desvio de recursos de segurança.
- 24 vulnerabilidades de execução remota de código.
- 9 vulnerabilidades de divulgação de informações.
- 3 vulnerabilidades de negação de serviço.
- 5 vulnerabilidades de falsificação.
- 5 Edge – vulnerabilidades do Chromium.

A contagem é um total de 59 falhas que não incluem cinco vulnerabilidades do Microsoft Edge (Chromium), duas falhas Microsoft no Electron e Autodesk.

2 VULNERABILIDADES DE ZERO DAY EXPLORADAS

O Patch Tuesday corrigiu duas vulnerabilidades de zero day, ambas exploradas em ataques e uma delas divulgada publicamente.

As duas vulnerabilidades de **zero day exploradas** nas atualizações são:

- **CVE-2023-36802:** Vulnerabilidade de elevação de privilégio do proxy do serviço de streaming da Microsoft. Esta vulnerabilidade permite que os atores obtenham privilégios de SYSTEM no sistema.

- **CVE-2023-36761:** Vulnerabilidade de divulgação de informações do Microsoft Word. Poderia ser utilizada para roubar hashes NTLM ao abrir um documento, inclusive no painel de visualização. Vale salientar que estas hashes podem ser quebradas para obter acesso a conta.

3 TABELA DAS VULNERABILIDADES CORRIGIDAS

Tag	CVE ID	CVE Title	Severity
.NET and Visual Studio	CVE-2023-36794	Visual Studio Remote Code Execution Vulnerability	Important
.NET and Visual Studio	CVE-2023-36796	Visual Studio Remote Code Execution Vulnerability	**Critical**
.NET and Visual Studio	CVE-2023-36792	Visual Studio Remote Code Execution Vulnerability	**Critical**
.NET and Visual Studio	CVE-2023-36793	Visual Studio Remote Code Execution Vulnerability	**Critical**
.NET Core & Visual Studio	CVE-2023-36799	.NET Core and Visual Studio Denial of Service Vulnerability	Important
.NET Framework	CVE-2023-36788	.NET Framework Remote Code Execution Vulnerability	Important
3D Builder	CVE-2023-36772	3D Builder Remote Code Execution Vulnerability	Important
3D Builder	CVE-2023-36771	3D Builder Remote Code Execution Vulnerability	Important
3D Builder	CVE-2023-36770	3D Builder Remote Code Execution Vulnerability	Important
3D Builder	CVE-2023-36773	3D Builder Remote Code Execution Vulnerability	Important
3D Viewer	CVE-2022-41303	AutoDesk: CVE-2022-41303 use-after-free vulnerability in Autodesk® FBX® SDK 2020 or prior	Important
3D Viewer	CVE-2023-36760	3D Viewer Remote Code Execution Vulnerability	Important
3D Viewer	CVE-2023-36740	3D Viewer Remote Code Execution Vulnerability	Important
3D Viewer	CVE-2023-36739	3D Viewer Remote Code Execution Vulnerability	Important
Azure DevOps	CVE-2023-33136	Azure DevOps Server Remote Code Execution Vulnerability	Important
Azure DevOps	CVE-2023-38155	Azure DevOps Server Remote Code Execution Vulnerability	Important
Azure HDInsights	CVE-2023-38156	Azure HDInsight Apache Ambari Elevation of Privilege Vulnerability	Important
Microsoft Azure Kubernetes Service	CVE-2023-29332	Microsoft Azure Kubernetes Service Elevation of Privilege Vulnerability	**Critical**
Microsoft Dynamics	CVE-2023-38164	Microsoft Dynamics 365 (on-premises) Cross-site Scripting Vulnerability	Important

Microsoft Dynamics	CVE-2023-36886	Microsoft Dynamics 365 (on-premises) Cross-site Scripting Vulnerability	Important
Microsoft Dynamics Finance & Operations	CVE-2023-36800	Dynamics Finance and Operations Cross-site Scripting Vulnerability	Important
Microsoft Edge (Chromium-based)	CVE-2023-4863	Chromium: CVE-2023-4863 Heap buffer overflow in WebP	Unknown
Microsoft Edge (Chromium-based)	CVE-2023-4763	Chromium: CVE-2023-4763 Use after free in Networks	Unknown
Microsoft Edge (Chromium-based)	CVE-2023-4761	Chromium: CVE-2023-4761 Out of bounds memory access in FedCM	Unknown
Microsoft Edge (Chromium-based)	CVE-2023-4764	Chromium: CVE-2023-4764 Incorrect security UI in BFCache	Unknown
Microsoft Edge (Chromium-based)	CVE-2023-4762	Chromium: CVE-2023-4762 Type Confusion in V8	Unknown
Microsoft Exchange Server	CVE-2023-36744	Microsoft Exchange Server Remote Code Execution Vulnerability	Important
Microsoft Exchange Server	CVE-2023-36756	Microsoft Exchange Server Remote Code Execution Vulnerability	Important
Microsoft Exchange Server	CVE-2023-36745	Microsoft Exchange Server Remote Code Execution Vulnerability	Important
Microsoft Exchange Server	CVE-2023-36777	Microsoft Exchange Server Information Disclosure Vulnerability	Important
Microsoft Exchange Server	CVE-2023-36757	Microsoft Exchange Server Spoofing Vulnerability	Important
Microsoft Identity Linux Broker	CVE-2023-36736	Microsoft Identity Linux Broker Remote Code Execution Vulnerability	Important
Microsoft Office	CVE-2023-36767	Microsoft Office Security Feature Bypass Vulnerability	Important
Microsoft Office	CVE-2023-36765	Microsoft Office Elevation of Privilege Vulnerability	Important
Microsoft Office	CVE-2023-41764	Microsoft Office Spoofing Vulnerability	Moderate
Microsoft Office Excel	CVE-2023-36766	Microsoft Excel Information Disclosure Vulnerability	Important
Microsoft Office Outlook	CVE-2023-36763	Microsoft Outlook Information Disclosure Vulnerability	Important
Microsoft Office SharePoint	CVE-2023-36764	Microsoft SharePoint Server Elevation of Privilege Vulnerability	Important
Microsoft Office Word	CVE-2023-36761	Microsoft Word Information Disclosure Vulnerability	Important
Microsoft Office Word	CVE-2023-36762	Microsoft Word Remote Code Execution Vulnerability	Important

Microsoft Streaming Service	CVE-2023-36802	Microsoft Streaming Service Proxy Elevation of Privilege Vulnerability	Important
Microsoft Windows Codecs Library	CVE-2023-38147	Windows Miracast Wireless Display Remote Code Execution Vulnerability	Important
Visual Studio	CVE-2023-36758	Visual Studio Elevation of Privilege Vulnerability	Important
Visual Studio	CVE-2023-36759	Visual Studio Elevation of Privilege Vulnerability	Important
Visual Studio Code	CVE-2023-36742	Visual Studio Code Remote Code Execution Vulnerability	Important
Visual Studio Code	CVE-2023-39956	Electron: CVE-2023-39956 -Visual Studio Code Remote Code Execution Vulnerability	Important
Windows Cloud Files Mini Filter Driver	CVE-2023-35355	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability	Important
Windows Common Log File System Driver	CVE-2023-38143	Windows Common Log File System Driver Elevation of Privilege Vulnerability	Important
Windows Common Log File System Driver	CVE-2023-38144	Windows Common Log File System Driver Elevation of Privilege Vulnerability	Important
Windows Defender	CVE-2023-38163	Windows Defender Attack Surface Reduction Security Feature Bypass	Important
Windows DHCP Server	CVE-2023-38152	DHCP Server Service Information Disclosure Vulnerability	Important
Windows DHCP Server	CVE-2023-38162	DHCP Server Service Denial of Service Vulnerability	Important
Windows DHCP Server	CVE-2023-36801	DHCP Server Service Information Disclosure Vulnerability	Important
Windows GDI	CVE-2023-36804	Windows GDI Elevation of Privilege Vulnerability	Important
Windows GDI	CVE-2023-38161	Windows GDI Elevation of Privilege Vulnerability	Important
Windows Internet Connection Sharing (ICS)	CVE-2023-38148	Internet Connection Sharing (ICS) Remote Code Execution Vulnerability	Critical
Windows Kernel	CVE-2023-38141	Windows Kernel Elevation of Privilege Vulnerability	Important
Windows Kernel	CVE-2023-38142	Windows Kernel Elevation of Privilege Vulnerability	Important
Windows Kernel	CVE-2023-38139	Windows Kernel Elevation of Privilege Vulnerability	Important
Windows Kernel	CVE-2023-38140	Windows Kernel Information Disclosure Vulnerability	Important

Windows Kernel	CVE-2023-38150	Windows Kernel Elevation of Privilege Vulnerability	Important
Windows Kernel	CVE-2023-36803	Windows Kernel Information Disclosure Vulnerability	Important
Windows Scripting	CVE-2023-36805	Windows MSHTML Platform Security Feature Bypass Vulnerability	Important
Windows TCP/IP	CVE-2023-38160	Windows TCP/IP Information Disclosure Vulnerability	Important
Windows TCP/IP	CVE-2023-38149	Windows TCP/IP Denial of Service Vulnerability	Important
Windows Themes	CVE-2023-38146	Windows Themes Remote Code Execution Vulnerability	Important

Tabela 1 – Listas das vulnerabilidades corrigidas no Patch.

4 RECOMENDAÇÕES

É altamente recomendado que os usuários dos sistemas operacionais Windows e seus Softwares realizem atualizações de seguranças divulgadas pela Microsoft.

5 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Boletim Microsoft – Patch Tuesday Setembro 2023**

heimdall
security research
A DIVISION OF ISH