ALERTA DE VULNERABILIDADE

Patch Tuesday de Abril de 2024

heimdall
security research
A DIVISION OF ISH

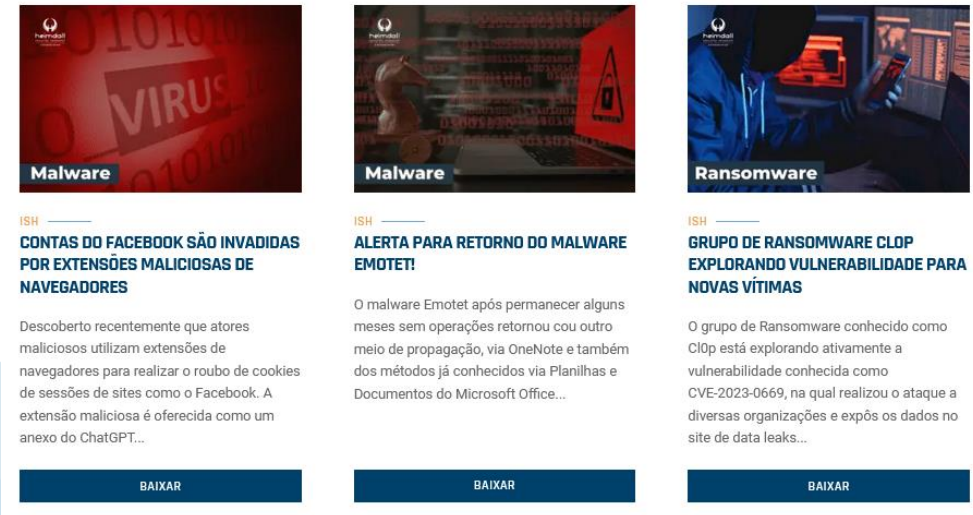
TLP: CLEAR

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 abril de 2024 da Microsoft, o qual incluiu atualizações de segurança para um total de 150 falhas e 67 falhas de execução remota de código. 03 falhas foram classificadas como críticas.

O número de bugs em cada categoria de vulnerabilidade é listado abaixo:

- 31 Vulnerabilidades de elevação de privilégio
- 29 Vulnerabilidades de desvio de recursos de segurança
- 67 Vulnerabilidades de execução remota de código
- 13 Vulnerabilidades de divulgação de informações
- 7 vulnerabilidades de negação de serviço
- 3 vulnerabilidades de falsificação

2 VULNERABILIDADES EXPLORADAS 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. Inicialmente, a Microsoft não reconheceu essas vulnerabilidades como sendo alvo de ataques ativos, porém a Sophos e a Trend Micro forneceram informações que confirmaram sua exploração em ataques recentes.

Segue um resumo das vulnerabilidades de *zero day* abordadas:

CVE-2024-26234 - Vulnerabilidade de falsificação de driver proxy

Segundo a Sophos, o CVE em questão está vinculado a um driver malicioso que possui uma assinatura válida do Microsoft Hardware Publisher, esse driver foi empregado para instalar um backdoor anteriormente identificado pela Stairwell. Christopher Budd, líder da equipe, informou ao BleepingComputer que drivers anteriores foram reportados à Microsoft, não resultando em um CVE, mas sim em um aviso emitido. Não está claro por que um CVE foi lançado para este driver no patch tuesday, a menos que tenha sido assinado por um certificado válido do Microsoft Hardware Publisher.

CVE-2024-29988 - Vulnerabilidade de desvio do recurso de segurança do prompt do SmartScreen

Esta falha é um desvio de patch para a falha CVE-2024-21412 (também um desvio de patch para CVE-2023-36025), que permite que anexos ignorem os prompts do Microsoft Defender Smartscreen quando o arquivo é aberto. Isso foi usado pelo grupo de hackers Water Hydra, com motivação financeira, para atingir fóruns de negociação forex e canais de negociação de ações do Telegram em ataques de spearphishing que implantaram o trojan de acesso remoto DarkMe (RAT).

3 ATUALIZAÇÕES DE SEGURANÇA DO PATCH TUESDAY

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

Tag	CVE ID	CVE Title	Severity
.NET and Visual Studio	CVE-2024-21409	.NET, .NET Framework, and Visual Studio Remote Code Execution Vulnerability	Important
Azure	CVE-2024-29993	Azure CycleCloud Elevation of Privilege Vulnerability	Important
Azure AI Search	CVE-2024-29063	Azure AI Search Information Disclosure Vulnerability	Important
Azure Arc	CVE-2024-28917	Azure Arc-enabled Kubernetes Extension Cluster-Scope Elevation of Privilege Vulnerability	Important
Azure Compute Gallery	CVE-2024-21424	Azure Compute Gallery Elevation of Privilege Vulnerability	Important
Azure Migrate	CVE-2024-26193	Azure Migrate Remote Code Execution Vulnerability	Important
Azure Monitor	CVE-2024-29989	Azure Monitor Agent Elevation of Privilege Vulnerability	Important
Azure Private 5G Core	CVE-2024-20685	Azure Private 5G Core Denial of Service Vulnerability	Moderate

Azure SDK	CVE-2024-29992	Azure Identity Library for .NET Information Disclosure Vulnerability	Moderate
Intel	CVE-2024-2201	Intel: CVE-2024-2201 Branch History Injection	Important
Internet Shortcut Files	CVE-2024-29988	SmartScreen Prompt Security Feature Bypass Vulnerability	Important
Mariner	CVE-2019-3816	Unknown	Unknown
Mariner	CVE-2019-3833	Unknown	Unknown
Microsoft Azure Kubernetes Service	CVE-2024-29990	Microsoft Azure Kubernetes Service Confidential Container Elevation of Privilege Vulnerability	Important
Microsoft Brokering File System	CVE-2024-28905	Microsoft Brokering File System Elevation of Privilege Vulnerability	Important
Microsoft Brokering File System	CVE-2024-28907	Microsoft Brokering File System Elevation of Privilege Vulnerability	Important

Microsoft Brokering File System	CVE-2024-26213	Microsoft Brokering File System Elevation of Privilege Vulnerability	Important
Microsoft Brokering File System	CVE-2024-28904	Microsoft Brokering File System Elevation of Privilege Vulnerability	Important
Microsoft Defender for IoT	CVE-2024-29055	Microsoft Defender for IoT Elevation of Privilege Vulnerability	Important
Microsoft Defender for IoT	CVE-2024-29053	Microsoft Defender for IoT Remote Code Execution Vulnerability	**Critical**
Microsoft Defender for IoT	CVE-2024-29054	Microsoft Defender for IoT Elevation of Privilege Vulnerability	Important
Microsoft Defender for IoT	CVE-2024-21324	Microsoft Defender for IoT Elevation of Privilege Vulnerability	Important
Microsoft Defender for IoT	CVE-2024-21323	Microsoft Defender for IoT Remote Code Execution Vulnerability	**Critical**
Microsoft Defender for IoT	CVE-2024-21322	Microsoft Defender for IoT Remote Code Execution Vulnerability	**Critical**
Microsoft Edge (Chromium-based)	CVE-2024-3156	Chromium: CVE-2024-3156 Inappropriate implementation in V8	Unknown

Microsoft Edge (Chromium-based)	CVE-2024-29049	Microsoft Edge (Chromium-based) Webview2 Spoofing Vulnerability	Moderate
Microsoft Edge (Chromium-based)	CVE-2024-29981	Microsoft Edge (Chromium-based) Spoofing Vulnerability	Low
Microsoft Edge (Chromium-based)	CVE-2024-3159	Chromium: CVE-2024-3159 Out of bounds memory access in V8	Unknown
Microsoft Edge (Chromium-based)	CVE-2024-3158	Chromium: CVE-2024-3158 Use after free in Bookmarks	Unknown
Microsoft Install Service	CVE-2024-26158	Microsoft Install Service Elevation of Privilege Vulnerability	Important
Microsoft Office Excel	CVE-2024-26257	Microsoft Excel Remote Code Execution Vulnerability	Important
Microsoft Office Outlook	CVE-2024-20670	Outlook for Windows Spoofing Vulnerability	Important
Microsoft Office SharePoint	CVE-2024-26251	Microsoft SharePoint Server Spoofing Vulnerability	Important
Microsoft WDAC ODBC Driver	CVE-2024-26214	Microsoft WDAC SQL Server ODBC Driver Remote Code Execution Vulnerability	Important
Microsoft WDAC OLE DB provider for SQL	CVE-2024-26244	Microsoft WDAC OLE DB Provider for SQL Server Remote Code Execution Vulnerability	Important

Microsoft WDAC OLE DB provider for SQL	CVE-2024-26210	Microsoft WDAC OLE DB Provider for SQL Server Remote Code Execution Vulnerability	Important
Role: DNS Server	CVE-2024-26233	Windows DNS Server Remote Code Execution Vulnerability	Important
Role: DNS Server	CVE-2024-26231	Windows DNS Server Remote Code Execution Vulnerability	Important
Role: DNS Server	CVE-2024-26227	Windows DNS Server Remote Code Execution Vulnerability	Important
Role: DNS Server	CVE-2024-26223	Windows DNS Server Remote Code Execution Vulnerability	Important
Role: DNS Server	CVE-2024-26221	Windows DNS Server Remote Code Execution Vulnerability	Important
Role: DNS Server	CVE-2024-26224	Windows DNS Server Remote Code Execution Vulnerability	Important
Role: DNS Server	CVE-2024-26222	Windows DNS Server Remote Code Execution Vulnerability	Important

Role: Windows Hyper-V	CVE-2024-29064	Windows Hyper-V Denial of Service Vulnerability	Important
SQL Server	CVE-2024-28937	Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability	Important
SQL Server	CVE-2024-28938	Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability	Important
SQL Server	CVE-2024-29044	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability	Important
SQL Server	CVE-2024-28935	Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability	Important
SQL Server	CVE-2024-28940	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability	Important
SQL Server	CVE-2024-28943	Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability	Important

SQL Server	CVE-2024-28941	Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability	Important
SQL Server	CVE-2024-28910	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability	Important
SQL Server	CVE-2024-28944	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability	Important
SQL Server	CVE-2024-28908	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability	Important
SQL Server	CVE-2024-28909	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability	Important
SQL Server	CVE-2024-29985	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability	Important
SQL Server	CVE-2024-28906	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability	Important
SQL Server	CVE-2024-28926	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability	Important

SQL Server	CVE-2024-28933	Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability	Important
SQL Server	CVE-2024-28934	Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability	Important
SQL Server	CVE-2024-28927	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability	Important
SQL Server	CVE-2024-28930	Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability	Important
SQL Server	CVE-2024-29046	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability	Important
SQL Server	CVE-2024-28932	Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability	Important
SQL Server	CVE-2024-29047	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability	Important
SQL Server	CVE-2024-28931	Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability	Important
SQL Server	CVE-2024-29984	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability	Important

SQL Server	CVE-2024-28929	Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability	Important
SQL Server	CVE-2024-28939	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability	Important
SQL Server	CVE-2024-28942	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability	Important
SQL Server	CVE-2024-29043	Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability	Important
SQL Server	CVE-2024-28936	Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability	Important
SQL Server	CVE-2024-29045	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability	Important
SQL Server	CVE-2024-28915	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability	Important
SQL Server	CVE-2024-28913	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability	Important

SQL Server	CVE-2024-28945	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability	Important
SQL Server	CVE-2024-29048	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability	Important
SQL Server	CVE-2024-28912	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability	Important
SQL Server	CVE-2024-28914	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability	Important
SQL Server	CVE-2024-29983	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability	Important
SQL Server	CVE-2024-28911	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability	Important
SQL Server	CVE-2024-29982	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability	Important
Windows Authentication Methods	CVE-2024-29056	Windows Authentication Elevation of Privilege Vulnerability	Important
Windows Authentication Methods	CVE-2024-21447	Windows Authentication Elevation of Privilege Vulnerability	Important

Windows BitLocker	CVE-2024-20665	BitLocker Security Feature Bypass Vulnerability	Important
Windows Compressed Folder	CVE-2024-26256	libarchive Remote Code Execution Vulnerability	Important
Windows Cryptographic Services	CVE-2024-26228	Windows Cryptographic Services Security Feature Bypass Vulnerability	Important
Windows Cryptographic Services	CVE-2024-29050	Windows Cryptographic Services Remote Code Execution Vulnerability	Important
Windows Defender Credential Guard	CVE-2024-26237	Windows Defender Credential Guard Elevation of Privilege Vulnerability	Important
Windows DHCP Server	CVE-2024-26212	DHCP Server Service Denial of Service Vulnerability	Important
Windows DHCP Server	CVE-2024-26215	DHCP Server Service Denial of Service Vulnerability	Important
Windows DHCP Server	CVE-2024-26195	DHCP Server Service Remote Code Execution Vulnerability	Important
Windows DHCP Server	CVE-2024-26202	DHCP Server Service Remote Code Execution Vulnerability	Important
Windows Distributed File System (DFS)	CVE-2024-29066	Windows Distributed File System (DFS) Remote Code Execution Vulnerability	Important
Windows Distributed File System (DFS)	CVE-2024-26226	Windows Distributed File System (DFS) Information Disclosure Vulnerability	Important
Windows DWM Core Library	CVE-2024-26172	Windows DWM Core Library Information	Important

		Disclosure Vulnerability	
Windows File Server Resource Management Service	CVE-2024-26216	Windows File Server Resource Management Service Elevation of Privilege Vulnerability	Important
Windows HTTP.sys	CVE-2024-26219	HTTP.sys Denial of Service Vulnerability	Important
Windows Internet Connection Sharing (ICS)	CVE-2024-26253	Windows rndismp6.sys Remote Code Execution Vulnerability	Important
Windows Internet Connection Sharing (ICS)	CVE-2024-26252	Windows rndismp6.sys Remote Code Execution Vulnerability	Important
Windows Kerberos	CVE-2024-26183	Windows Kerberos Denial of Service Vulnerability	Important
Windows Kerberos	CVE-2024-26248	Windows Kerberos Elevation of Privilege Vulnerability	Important
Windows Kernel	CVE-2024-20693	Windows Kernel Elevation of Privilege Vulnerability	Important
Windows Kernel	CVE-2024-26245	Windows SMB Elevation of Privilege Vulnerability	Important
Windows Kernel	CVE-2024-26229	Windows CSC Service Elevation of Privilege Vulnerability	Important
Windows Kernel	CVE-2024-26218	Windows Kernel Elevation of Privilege Vulnerability	Important
Windows Local Security Authority Subsystem Service (LSASS)	CVE-2024-26209	Microsoft Local Security Authority Subsystem Service Information Disclosure Vulnerability	Important
Windows Message Queuing	CVE-2024-26232	Microsoft Message Queuing (MSMQ)	Important

		Remote Code Execution Vulnerability	
Windows Message Queuing	CVE-2024-26208	Microsoft Message Queuing (MSMQ) Remote Code Execution Vulnerability	Important
Windows Mobile Hotspot	CVE-2024-26220	Windows Mobile Hotspot Information Disclosure Vulnerability	Important
Windows Proxy Driver	CVE-2024-26234	Proxy Driver Spoofing Vulnerability	Important
Windows Remote Access Connection Manager	CVE-2024-28902	Windows Remote Access Connection Manager Information Disclosure Vulnerability	Important
Windows Remote Access Connection Manager	CVE-2024-28900	Windows Remote Access Connection Manager Information Disclosure Vulnerability	Important
Windows Remote Access Connection Manager	CVE-2024-28901	Windows Remote Access Connection Manager Information Disclosure Vulnerability	Important
Windows Remote Access Connection Manager	CVE-2024-26255	Windows Remote Access Connection Manager Information Disclosure Vulnerability	Important
Windows Remote Access Connection Manager	CVE-2024-26230	Windows Telephony Server Elevation of Privilege Vulnerability	Important
Windows Remote Access Connection Manager	CVE-2024-26239	Windows Telephony Server Elevation of Privilege Vulnerability	Important
Windows Remote Access Connection Manager	CVE-2024-26207	Windows Remote Access Connection Manager Information	Important

		Disclosure Vulnerability	
Windows Remote Access Connection Manager	CVE-2024-26217	Windows Remote Access Connection Manager Information Disclosure Vulnerability	Important
Windows Remote Access Connection Manager	CVE-2024-26211	Windows Remote Access Connection Manager Elevation of Privilege Vulnerability	Important
Windows Remote Procedure Call	CVE-2024-20678	Remote Procedure Call Runtime Remote Code Execution Vulnerability	Important
Windows Routing and Remote Access Service (RRAS)	CVE-2024-26200	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	Important
Windows Routing and Remote Access Service (RRAS)	CVE-2024-26179	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	Important
Windows Routing and Remote Access Service (RRAS)	CVE-2024-26205	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	Important
Windows Secure Boot	CVE-2024-29061	Secure Boot Security Feature Bypass Vulnerability	Important
Windows Secure Boot	CVE-2024-28921	Secure Boot Security Feature Bypass Vulnerability	Important
Windows Secure Boot	CVE-2024-20689	Secure Boot Security Feature Bypass Vulnerability	Important
Windows Secure Boot	CVE-2024-26250	Secure Boot Security Feature Bypass Vulnerability	Important
Windows Secure Boot	CVE-2024-28922	Secure Boot Security Feature	Important

		Bypass Vulnerability	
Windows Secure Boot	CVE-2024-29062	Secure Boot Security Feature Bypass Vulnerability	Important
Windows Secure Boot	CVE-2024-20669	Secure Boot Security Feature Bypass Vulnerability	Important
Windows Secure Boot	CVE-2024-28898	Secure Boot Security Feature Bypass Vulnerability	Important
Windows Secure Boot	CVE-2024-20688	Secure Boot Security Feature Bypass Vulnerability	Important
Windows Secure Boot	CVE-2024-23593	Lenovo: CVE-2024-23593 Zero Out Boot Manager and drop to UEFI Shell	Important
Windows Secure Boot	CVE-2024-28896	Secure Boot Security Feature Bypass Vulnerability	Important
Windows Secure Boot	CVE-2024-28919	Secure Boot Security Feature Bypass Vulnerability	Important
Windows Secure Boot	CVE-2024-23594	Lenovo: CVE-2024-23594 Stack Buffer Overflow in LenovoBT.efi	Important
Windows Secure Boot	CVE-2024-28923	Secure Boot Security Feature Bypass Vulnerability	Important
Windows Secure Boot	CVE-2024-28903	Secure Boot Security Feature Bypass Vulnerability	Important
Windows Secure Boot	CVE-2024-26189	Secure Boot Security Feature Bypass Vulnerability	Important
Windows Secure Boot	CVE-2024-26240	Secure Boot Security Feature Bypass Vulnerability	Important
Windows Secure Boot	CVE-2024-28924	Secure Boot Security Feature Bypass Vulnerability	Important

Windows Secure Boot	CVE-2024-28897	Secure Boot Security Feature Bypass Vulnerability	Important
Windows Secure Boot	CVE-2024-28925	Secure Boot Security Feature Bypass Vulnerability	Important
Windows Secure Boot	CVE-2024-26175	Secure Boot Security Feature Bypass Vulnerability	Important
Windows Secure Boot	CVE-2024-28920	Secure Boot Security Feature Bypass Vulnerability	Important
Windows Secure Boot	CVE-2024-26194	Secure Boot Security Feature Bypass Vulnerability	Important
Windows Secure Boot	CVE-2024-26180	Secure Boot Security Feature Bypass Vulnerability	Important
Windows Secure Boot	CVE-2024-26171	Secure Boot Security Feature Bypass Vulnerability	Important
Windows Secure Boot	CVE-2024-26168	Secure Boot Security Feature Bypass Vulnerability	Important
Windows Storage	CVE-2024-29052	Windows Storage Elevation of Privilege Vulnerability	Important
Windows Telephony Server	CVE-2024-26242	Windows Telephony Server Elevation of Privilege Vulnerability	Important
Windows Update Stack	CVE-2024-26236	Windows Update Stack Elevation of Privilege Vulnerability	Important
Windows Update Stack	CVE-2024-26235	Windows Update Stack Elevation of Privilege Vulnerability	Important
Windows USB Print Driver	CVE-2024-26243	Windows USB Print Driver Elevation of Privilege Vulnerability	Important

Windows Virtual Machine Bus	CVE-2024-26254	Microsoft Virtual Machine Bus (VMBus) Denial of Service Vulnerability	Important
Windows Win32K - ICOMP	CVE-2024-26241	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**


heimdall
security research
A DIVISION OF ISH