



BOLETIM DE SEGURANÇA

**CISA alerta sobre vulnerabilidade do Windows explorada
em ataques de malware**



Acesse boletins diários sobre agentes de ameaças, *malwares*, indicadores de comprometimentos, TTPs e outras informações no *site* da ISH.

[Boletins de Segurança – Heimdall](#)



ISH

CONTAS DO FACEBOOK SÃO INVADIDAS POR EXTENSÕES MALICIOSAS DE NAVEGADORES

Descoberto recentemente que atores maliciosos utilizam extensões de navegadores para realizar o roubo de cookies de sessões de sites como o Facebook. A extensão maliciosa é oferecida como um anexo do ChatGPT...

BAIXAR



ISH

ALERTA PARA RETORNO DO MALWARE EMOTET!

O malware Emotet após permanecer alguns meses sem operações retornou com outro meio de propagação, via OneNote e também dos métodos já conhecidos via Planilhas e Documentos do Microsoft Office...

BAIXAR



ISH

GRUPO DE RANSOMWARE CLOP EXPLORANDO VULNERABILIDADE PARA NOVAS VÍTIMAS

O grupo de Ransomware conhecido como Clop está explorando ativamente a vulnerabilidade conhecida como CVE-2023-0669, na qual realizou o ataque a diversas organizações e expôs os dados no site de data leaks...

BAIXAR

SUMÁRIO

1	Sumário Executivo	5
2	Informações sobre a vulnerabilidade	6
3	Vulnerabilidades adicionadas ao KEV-CISA.....	7
4	Recomendações.....	8
5	Referências	9
6	Autores.....	10

LISTA DE FIGURAS

Figura 1 – Vulnerabilidades no catálogo KEV-CISA..... 7

1 SUMÁRIO EXECUTIVO

A Agência de Segurança Cibernética e Infraestrutura dos EUA (CISA) emitiu um alerta de segurança para agências federais a protegerem seus sistemas contra a vulnerabilidade *zero day* [CVE-2024-43461](#) no MSHTML do Windows. Esta falha, recentemente corrigida, foi explorada pelo grupo de hackers Void Banshee APT.

2 INFORMAÇÕES SOBRE A VULNERABILIDADE


A vulnerabilidade identificada como CVE-2024-43461 categorizada como alta foi revelada durante o Patch Tuesday deste mês. Inicialmente, a Microsoft afirmou que a falha não havia sido explorada em ataques. No entanto, na sexta-feira, a empresa atualizou seu aviso, confirmando que a vulnerabilidade foi explorada antes de ser corrigida. A Microsoft informou que os invasores utilizaram a falha antes de julho de 2024, em conjunto com o CVE-2024-38112, outro bug de falsificação de MSHTML, como parte de uma cadeia de exploração. Em julho de 2024, foi lançada uma correção para a vulnerabilidade CVE-2024-38112, interrompendo a cadeia de ataque. Para proteção completa, os clientes devem aplicar as atualizações de segurança de julho e setembro de 2024. Peter Girnus, pesquisador da Trend Micro Zero Day Initiative (ZDI), relatou que hackers do grupo Void Banshee exploraram essa falha em ataques zero days para instalar malware de roubo de informações.

A vulnerabilidade permite que invasores de forma remota executem código arbitrário em sistemas Windows não corrigidos, enganando os alvos para que visitem páginas da web maliciosas e/ou abram arquivos infectados. Segundo o ZDI, a falha está na maneira como o Internet Explorer avisa o usuário após o download de um arquivo, ocultando a extensão real e fazendo o usuário acreditar que o arquivo é inofensivo. Isso permite que invasores executem código no contexto do usuário atual. Os atores maliciosos usaram exploits para entregar arquivos HTA maliciosos disfarçados de documentos PDF, utilizando caracteres de espaço em branco braille (%E2%A0%80) para esconder a extensão .hta. O malware Atlantida, usado nesses ataques, pode roubar senhas, cookies de autenticação e carteiras de criptomoedas de dispositivos infectados, conforme revelado pela Check Point Research e Trend Micro. O grupo Void Banshee, é conhecido por atacar organizações na América do Norte, Europa e Sudeste Asiático para obter ganhos financeiros e roubar dados.

3 VULNERABILIDADE ADICIONADA AO KEV-CISA

A agência de segurança cibernética (CISA) adicionou a falha ao seu Catálogo de Vulnerabilidades Exploradas Conhecidas (KEV), dizendo que tal vulnerabilidade é “um vetor de ataque frequente para atores cibernéticos maliciosos”.

MICROSOFT | WINDOWS

 [CVE-2024-43461](#) CV

Vulnerabilidade de falsificação da plataforma Microsoft Windows MSHTML: *A plataforma Microsoft Windows MSHTML contém uma vulnerabilidade de representação incorreta de informações críticas na interface do usuário (UI) que permite que um invasor falsifique uma página da web. Essa vulnerabilidade foi explorada em conjunto com CVE-2024-38112.*

Conhecido por ser usado em campanhas de ransomware? **Desconhecido**

Ação: Aplique medidas de mitigação conforme as instruções do fornecedor ou interrompa o uso do produto se medidas de mitigação não estiverem disponíveis.

- **Data adicionada:** 2024-09-16
- **Data de vencimento:** 2024-10-07

Figura 1 – Vulnerabilidade no catálogo KEV-CISA.

4 RECOMENDAÇÕES

Aplicar as atualizações de segurança

- Certifique-se de que todas as atualizações de segurança mais recentes da Microsoft, especialmente as de julho e setembro de 2024, estejam instaladas.

Desativar o MSHTML (Trident)

- Se possível, desative o uso do motor de navegador MSHTML (Trident) em sistemas que não necessitam dele para reduzir a superfície de ataque.

Educação e conscientização dos usuários

- Instrua os usuários a não clicarem em links desconhecidos ou suspeitos e a evitarem abrir anexos de e-mails de remetentes não confiáveis.

Implementar filtros de e-mail

- Utilize filtros de e-mail para bloquear mensagens que contenham links ou anexos potencialmente maliciosos.

Monitoramento e detecção de ameaças

- Implemente soluções de monitoramento e detecção de ameaças para identificar atividades suspeitas relacionadas a essa vulnerabilidade.

Revisar e atualizar políticas de segurança

- Revise e atualize as políticas de segurança para garantir que estejam alinhadas com as melhores práticas de mitigação de vulnerabilidades.

Backup regular de dados

- Realize backups regulares dos dados críticos para garantir que possam ser restaurados em caso de um ataque bem-sucedido.

5 REFERÊNCIAS

- Heimdall by ISH Tecnologia
- [Microsoft](#)
- [Bleepingcomputer](#)
- [CISA](#)
- [NVD](#)

6 AUTORES

- Leonardo Oliveira Silva



heimdall
security research

A DIVISION OF ISH