BOLETIM DE SEGURANÇA

Vulnerabilidade de execução remota de código TCP/IP do Windows, afetando todos os sistemas com IPv6 habilitado

heimdall
security research
A DIVISION OF ISH

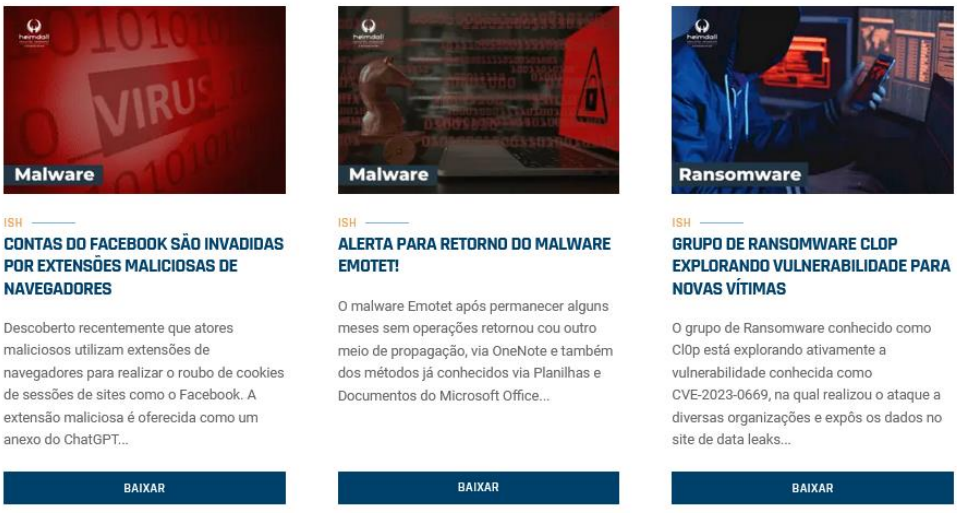
TLP: CLEAR

Receba alertas e informações sobre segurança cibernética e ameaças rapidamente, por meio do nosso **X**.

[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

1 SUMÁRIO EXECUTIVO

A Microsoft emitiu um alerta recomendando que os clientes corrijam a vulnerabilidade **CVE-2024-38063** crítica de execução remota de código (RCE) no protocolo TCP/IP, que possui alta probabilidade de exploração. Essa falha afeta todos os sistemas Windows que utilizam o IPv6, o qual é ativado por padrão, o mesmo é causado por uma fraqueza de *Integer Underflow*, que os invasores podem explorar para disparar estouros de buffer que podem ser usados para executar código arbitrário em sistemas vulneráveis.

2 SISTEMAS E VERSÕES AFETADAS

Abaixo segue os sistemas e versões da Microsoft afetados pela vulnerabilidade segurança

- *Windows Server 2012 R2*
- *Windows Server 2012 (Server Core installation)*
- *Windows Server 2012*
- *Windows Server 2008 R2 for x64based Systems Service Pack 1 (Server Core installation)*
- *Windows Server 2008 R2 for x64based Systems Service Pack 1*
- *Windows Server 2008 for x64based Systems Service Pack 2 (Server Core installation)*
- *Windows Server 2008 for x64based Systems Service Pack 2*
- *Windows Server 2008 for 32bit Systems Service Pack 2 (Server Core installation)*
- *Windows Server 2008 for 32bit Systems Service Pack 2*
- *Windows Server 2016 (Server Core installation)*
- *Windows Server 2016*
- *Windows 10 Version 1607 for x64based Systems*
- *Windows 10 Version 1607 for 32bit Systems*
- *Windows 10 for x64based Systems*
- *Windows 10 for 32bit Systems*
- *Windows Server 2022, 23H2 Edition (Server Core installation)*
- *Windows 11 Version 23H2 for x64based Systems*
- *Windows 11 Version 23H2 for ARM64based Systems*
- *Windows 10 Version 22H2 for 32bit Systems*
- *Windows 10 Version 22H2 for ARM64based Systems*
- *Windows 10 Version 22H2 for x64based Systems*
- *Windows 11 Version 22H2 for x64based Systems*
- *Windows 11 Version 22H2 for ARM64based Systems*
- *Windows 10 Version 21H2 for x64based Systems*
- *Windows 10 Version 21H2 for ARM64based Systems*
- *Windows 10 Version 21H2 for 32bit Systems*
- *Windows 11 version 21H2 for ARM64based Systems*
- *Windows 11 version 21H2 for x64based Systems*
- *Windows Server 2022 (Server Core installation)*
- *Windows Server 2022*
- *Windows Server 2019 (Server Core installation)*
- *Windows Server 2019*
- *Windows 10 Version 1809 for ARM64based Systems*
- *Windows 10 Version 1809 for x64based Systems*

- *Windows 10 Version 1809 for 32bit Systems*

3 RECOMENDAÇÕES

A Microsoft recomenda fortemente a instalação do patch de correção para a falha, o qual foi disponibilizado em seu Patch Tuesday.

- **Monitoramento contínuo**: Implementar e manter práticas de monitoramento contínuo para detectar e responder rapidamente a possíveis tentativas de exploração.

4 REFERÊNCIAS

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

5 AUTORES

- **Ismael Pereira Rocha**

heimdall
security research
A DIVISION OF ISH