BOLETIM DE SEGURANÇA

Microsoft corrige vulnerabilidade grave explorada pelo Lazarus Group

heimdall
security research
A DIVISION OF ISH

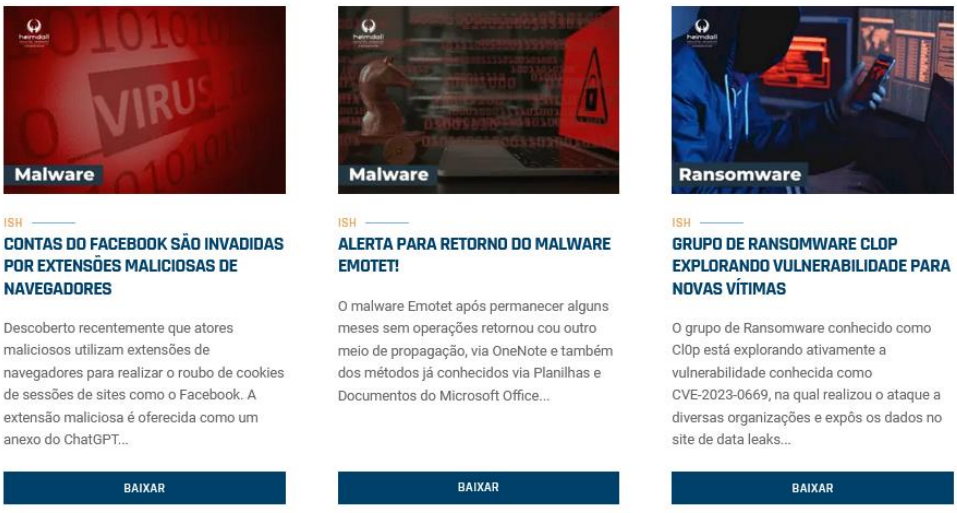
TLP: CLEAR

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]

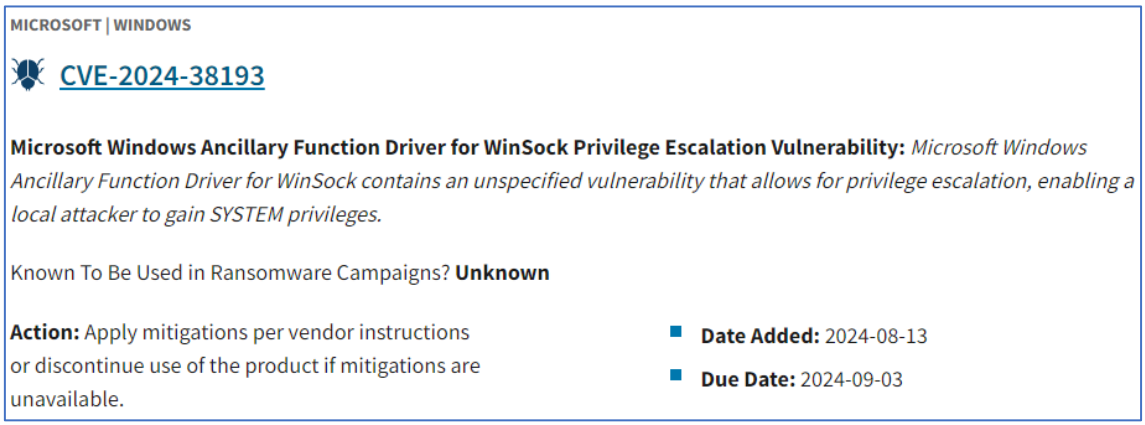


SUMÁRIO

LISTA DE FIGURAS

1 SUMÁRIO EXECUTIVO

Uma vulnerabilidade de segurança no Microsoft Windows, recentemente corrigida, foi explorada como um zero day pelo Lazarus Group, um grupo de hackers patrocinado pelo Estado e afiliado à Coreia do Norte.


MICROSOFT | WINDOWS

CVE-2024-38193

Microsoft Windows Ancillary Function Driver for WinSock Privilege Escalation Vulnerability: *Microsoft Windows Ancillary Function Driver for WinSock contains an unspecified vulnerability that allows for privilege escalation, enabling a local attacker to gain SYSTEM privileges.*

Known To Be Used in Ransomware Campaigns? **Unknown**

Action: Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.

- **Date Added:** 2024-08-13
- **Due Date:** 2024-09-03

Figura 1 – Vulnerabilidade no Catalogo KEV-CISA.

2 INFORMAÇÕES SOBRE A VULNERABILIDADE

A Vulnerabilidade CVE-2024-38193,um bug de escalonamento de privilégios no Windows Ancillary Function Driver (AFD.sys) para WinSock. Segundo a Microsoft, um invasor que explorasse essa vulnerabilidade com sucesso poderia obter privilégios de SISTEMA. A falha foi corrigida pela Microsoft na atualização mensal Patch Tuesday da semana passada.

Pesquisadores da Gen Digital, identificaram e relataram a vulnerabilidade. Segundo a empresa, a falha foi detectada no início de junho de 2024 e permitiu acesso não autorizado a partes críticas do sistema. A vulnerabilidade possibilitou que invasores contornassem as medidas de segurança padrão e acessassem áreas restritas do sistema, inacessíveis para a maioria dos usuários e administradores. Também foi destacado que os ataques utilizaram um rootkit chamado FudModule para evitar a detecção. Embora os detalhes técnicos das intrusões ainda sejam desconhecidos, a vulnerabilidade é semelhante a uma falha de escalonamento de privilégios corrigida pela Microsoft em fevereiro de 2024, que também foi explorada pelo Lazarus Group para neutralizar o FudModule.

Essa exploração envolveu a CVE-2024-21338, uma vulnerabilidade no kernel do Windows relacionada ao driver AppLocker (appid.sys). Essa falha permite a execução de código arbitrário, contornando todas as verificações de segurança e permitindo a execução do rootkit FudModule. Os ataques se destacam por irem além do método BYOVD, explorando uma vulnerabilidade em um driver já presente em um host Windows, ao invés de introduzir um driver vulnerável para burlar as medidas de segurança.

Relatórios anteriores da Avast indicam que o rootkit é distribuído através de um trojan de acesso remoto chamado Kaolin RAT. A empresa tcheca observou que o FudModule está apenas parcialmente integrado ao ecossistema de malware do Lazarus, destacando que o grupo Lazarus utiliza o rootkit com cautela, ativando-o apenas quando necessário e em situações específicas.

3 RECOMENDAÇÕES

Atualização Imediata

- Aplique a atualização de segurança fornecida pela Microsoft para corrigir a vulnerabilidade no driver Windows Ancillary Function (AFD.sys).

Monitoramento Contínuo

- Monitore continuamente as redes e sistemas para atividades suspeitas, especialmente aquelas relacionadas a contas com privilégios elevados.

Desativação de SSHv1

- Desative o suporte ao SSHv1 e permita apenas o uso do SSHv2 para evitar o uso de algoritmos antigos e vulneráveis.

Revisão de Privilégios

- Revise e restrinja os privilégios de contas de usuário para minimizar o impacto potencial de uma exploração bem-sucedida.

Implementação de Políticas de Segurança

- Estabeleça políticas de segurança rigorosas para a instalação e uso de drivers, evitando o método “Bring Your Own Vulnerable Driver” (BYOVD).

Backup Regular

- Realize backups regulares dos dados críticos para garantir a recuperação em caso de comprometimento do sistema.

Educação e Treinamento

- Eduque e treine os funcionários sobre práticas de segurança cibernética e como identificar possíveis ameaças.

4 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Microsoft**
- **Thehackernews**

5 AUTORES

- **Leonardo Oliveira Silva**

heimdall
security research
A DIVISION OF ISH