BOLETIM DE SEGURANÇA

Microsoft alerta sobre falhas de controladores de domínio e correções

heimdall
security research
A DIVISION OF ISH

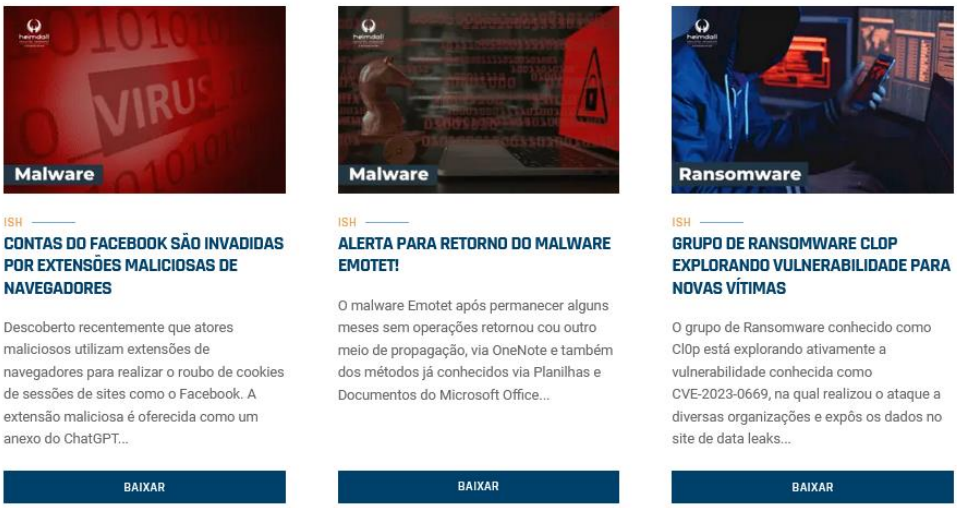
TLP: CLEAR

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 recentemente confirmou que um problema resultante em falhas nos controladores de domínio do Windows, é causado por um vazamento de memória. Este vazamento foi introduzido com as atualizações de segurança do Windows Server em março de 2024. Segundo o alerta informado pelos administradores, após a instalação das atualizações *KB5035855* e *KB5035857* do Windows Server lançadas no Patch Tuesday, os controladores de domínio com as atualizações mais recentes travariam e reinicializariam devido ao aumento do uso de memória LSASS.

2 INFORMAÇÕES SOBRE O PROBLEMA

Após a implementação das atualizações de março, tanto do Exchange quanto do Windows Server, foi observado um aumento contínuo no consumo de memória LSASS nos DCs, levando-os à falha. Ainda há problemas de vazamento de memória com lsass.exe nos controladores de domínio (core 2016, 2022 com DE e controladores de domínio core 2022). Isso resultou em uma paralisação, pois todos os controladores de domínio travaram durante o fim de semana. Os problemas identificados foram o crescimento do consumo de memória pelo processo lsass.exe após a instalação das atualizações KB5035855 (para Servidor 2016) e KB5035857 (para Servidor 2022). Isso levou ao esgotamento de toda a memória física e virtual, fazendo com que a máquina travasse.

A atualização KB5035855 é uma atualização cumulativa para o Windows Server 2016, sendo lançada em 12 de março de 2024 e aborda questões de segurança para o sistema operacional Windows.

A atualização KB5035857 é uma atualização cumulativa para o Windows Server 2022. Foi lançada em 12 de março de 2024 e aborda questões de segurança para o sistema operacional Windows.

Estas atualizações de segurança incluem melhorias e ao instalar esses KBs, são feitas melhorias diversas na funcionalidade interna do sistema operacional. Nenhum problema adicional foi documentado para esta versão.

3 MICROSOFT LANÇA NOVAS ATUALIZAÇÕES PARA CORREÇÕES

Devido a problemas causados por as atualizações acima, problemas como: travamentos devido a altos consumos de memória. A Microsoft lançou as seguintes atualizações cumulativas de emergência do Windows Server que devem corrigir o vazamento de memória LSASS e evitar que os servidores afetados travem e reiniciem:

- **Servidor Windows 2022:** KB5037422
- **Servidor Windows 2019:** KB5037425
- **Servidor Windows 2016:** KB5037423
- **Servidor Windows 2012 R2:** KB5037426

Esta atualização aborda um problema conhecido que afeta o Serviço de Subsistema de Autoridade de Segurança Local (LSASS). Ela pode vazar memória em controladores de domínio (DCs)", explica a empresa. O vazamento ocorre quando DCs do Active Directory locais e baseados em nuvem processam solicitações de autenticação Kerberos. Esse vazamento substancial pode causar uso excessivo de memória. Por causa disso, o LSASS pode parar de responder e os DCs serão reiniciados quando você não espera. "

4 REFERÊNCIAS

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

heimdall
security research
A DIVISION OF ISH