Várias explorações de dia zero descobrem que ignoram o BitLocker, expo

Data: 2025-08-09 12:47:04

Autor: Inteligência Against Invaders

Inteligência Against Invaders

2025-08-09 07:42

Pesquisadores de segurança da Microsoft descobriram quatro vulnerabilidades críticas em Windows BitLocker Isso pode permitir que invasores com acesso físico ignorem o sistema de criptografia e extraiam dados confidenciais.

As descobertas, reveladas em uma pesquisa apelidada de “BitUnlocker”, demonstram métodos sofisticados de ataque direcionados ao Windows Recovery Environment (WinRE) para contornar a principal tecnologia de proteção de dados da Microsoft.

Falhas de segurança visam o ambiente de recuperação do Windows

As vulnerabilidades, descobertas por Alon Leviev e Netanel Ben Simon, da equipe de Pesquisa Ofensiva e Engenharia de Segurança (MORSE) da Microsoft, exploram pontos fracos na forma como o WinRE processa arquivos e configurações externas.

Os pesquisadores identificaram quatro vetores de ataque distintos que permitem acesso não autorizado a sistemas protegidos pelo BitLocker:

- **CVE-2025-48800** permite que os invasores ignorem a validação do WIM (Windows Imaging Format) manipulando o ponteiro de deslocamento do arquivo Boot.sdi, fazendo com que o sistema inicialize um ambiente de recuperação não confiável enquanto valida um confiável.
- **CVE-2025-48003** As explorações ReAgent.xml análise para agendar operações maliciosas, incluindo o lançamento de tttracer.exe para executar prompts de comando com acesso total ao sistema.
- **CVE-2025-48804** aproveita a validação de confiança do aplicativo WinRE utilizando o SetupPlatform.exe pré-registrado para obter acesso persistente à linha de comando por meio de atalhos de teclado.
- **CVE-2025-48818** direciona a análise BCD (Dados de Configuração de Inicialização) para redirecionar o local do sistema operacional de destino do WinRE, permitindo a exploração de Redefinição de Botão para descriptografar volumes do BitLocker.

A pesquisa Revela que o WinRE, projetado como uma plataforma de recuperação para problemas críticos do sistema, cria inadvertidamente uma superfície de ataque ao analisar arquivos de configuração de volumes desprotegidos.

Os invasores podem manipular esses arquivos externos para obter privilégios elevados e acessar dados criptografados sem acionar os mecanismos de proteção padrão do BitLocker.

Microsoft responde com patches de segurança de julho de 2025

A Microsoft abordou todas as quatro vulnerabilidades como parte de seu Atualização de julho de 2025 , emitindo atualizações de segurança abrangentes nas versões afetadas do Windows.

Os patches são direcionados às edições Windows 10 (versões 1607, 21H2, 22H2), Windows 11 (versões 22H2, 23H2, 24H2) e Windows Server (2016, 2022, 2025).

As atualizações de segurança KB5062552, KB5062553, KB5062554 e KB5062560 abordam especificamente as vulnerabilidades do BitLocker, com as organizações instadas a priorizar a implantação imediata.

As vulnerabilidades carregam pontuações CVSS que variam de 6,8 a 8,1, com a Microsoft avaliando a exploração como “mais provável” para várias das falhas.

As descobertas da equipe de pesquisa foram programadas para apresentação na Black Hat USA 2025 em Las Vegas, destacando a importância das descobertas na comunidade de segurança cibernética.

A apresentação, intitulada “BitUnlocker: Aproveitando a recuperação do Windows para extrair segredos do BitLocker”, demonstra a análise abrangente dos pesquisadores sobre a arquitetura de segurança e as metodologias de ataque do WinRE.

Estratégias de proteção aprimoradas e impacto no setor

Além de aplicar os patches de segurança, Microsoft recomenda a implementação de contramedidas adicionais do BitLocker para fortalecer a proteção contra ataques físicos.

As organizações devem habilitar TPM+PIN para autenticação de pré-inicialização, que adiciona uma camada de autenticação adicional antes da inicialização do sistema, reduzindo significativamente o risco de tentativas de bypass físico.

A Microsoft também aconselha habilitar a mitigação REVISE para proteção anti-reversão, o que impede que os invasores façam downgrade para estados vulneráveis do sistema.

Essas proteções aprimoradas funcionam em conjunto com os patches de segurança para fornecer defesa abrangente contra os vetores de ataque identificados.

As descobertas ressaltam a importância de estratégias de defesa em profundidade para proteção de dados, particularmente em cenários que envolvem acesso a dispositivos físicos.

Embora o BitLocker continue sendo uma solução de criptografia robusta, a pesquisa demonstra que

mesmo sistemas de segurança sofisticados exigem avaliação e melhoria contínuas para lidar com vetores de ameaças emergentes.

A pesquisa do BitUnlocker representa uma contribuição significativa para a compreensão das técnicas de desvio de criptografia e reforça o papel crítico da segurança interna equipes de pesquisa na identificação e tratamento de vulnerabilidades antes que possam ser exploradas de forma maliciosa.

Organizações que dependem do BitLocker para Proteção de dados deve priorizar a aplicação das atualizações de segurança de julho de 2025 enquanto implementa as medidas de segurança adicionais recomendadas para manter uma proteção robusta contra ataques físicos.

Ache esta notícia interessante! Siga-nos no Google Notícias**,**LinkedIn**, &**X**para obter atualizações instantâneas!**