0 Clique com a vulnerabilidade Linux Kernel KSMBD permite a execução d

Data: 2025-09-16 07:19:06

Autor: Inteligência Against Invaders

Uma vulnerabilidade recente no módulo KSMBD do kernel Linux permite que um invasor execute o

código arbitrário em um sistema de destino sem qualquer interação do usuário.

O KSMBD é um servidor SMB3 em espaço de kernel que lida com o compartilhamento de arquivos de rede. Pesquisadores demonstrado Uma exploração estável contra o KSMBD no Linux 6.1.45, alcançando a execução do código remoto (RCE) com uma taxa de sucesso acima de 95 %.

A exploração aproveita dois CVEs conhecidos, corrigidos pela iniciativa do dia zero no início de 2024 e no final de 2023.

No primeiro estágio, um excesso de heap não autenticado (CVE-2023-52440) ocorre durante a autenticação NTLM.

Ao criar uma chave de sessão de grandes dimensões Blob em uma mensagem SMB2_SESSH_SETUP, a exploração força um excesso de slub controlado em uma alocação Kmalloc-512.

Esse transbordamento serve como um primitivo “WriteHeap”, permitindo que o atacante corrompe a memória do kernel adjacente sem autenticação.

Um segundo bug autenticado (CVE-2023-4130) nos atributos estendidos (EA) o analisador fornece, em seguida, fornece uma leitura fora do limite primitiva. Ao criar um tampão de EA malicioso, o invasor vaza o conteúdo de heap arbitrário através de metadados XATTR, equivalente a um primitivo “writeleak”.

Abuso de layout de heap e desvio KASLR

A combinação dessas primitivas permite uma corrente completa. O vazamento revela os ponteiros do kernel e ignora o KASLR lendo ponteiros de uma laje Kmalloc-1K que mantém objetos de conexão KSMBD.

Os pesquisadores pulverizam objetos do kernel abrindo várias conexões e sessões de SMB e acionam repetidamente o transbordamento até que uma conexão seja corrompida. Eles usam um loop guiado de spray e check para localizar com segurança a vítima de transbordamento e as dicas vazadas.

Com o desvio do KASLR, o atacante constrói os gadgets do kernel ROP para sequestrar o sessão do sessão.

Um primitivo livre arbitrário faz com que o pedaço de heap de uma sessão se sobreponha a um objeto de conexão, permitindo a substituição de ponteiros de função no Kmalloc-1k.

Finalmente, uma solicitação de SMB cuidadosamente criada aloca um grande pedaço contendo uma cadeia ROP. Essa cadeia gira a pilha na memória controlada, configura argumentos e callscall_usermodehelperto inicia um shell reverso no modo de usuário.

Um gadget do sono segura o fio do kernel vivo, impedindo a falha do sistema. O KSMBD é frequentemente desativado na produção, limitando o impacto generalizado.

No entanto, qualquer sistema que executa um kernel 6.1.x desatualizado com KSMBD ativado e exposto a redes não confiáveis ??é vulnerável.

[VÍDEO REMOVIDO]*Exploração de demonstração de ponta a ponta*

Os administradores do sistema devem atualizar para o kernel 6.1.46 ou posterior, onde ambos os CVEs são backported e corrigidos.

A ativação das opções de endurecimento padrão (SMEP, SMAP, KPTI, Freelista de laje aleatória) reduz a confiabilidade da exploração, mas não elimina completamente a ameaça.

Esta exploração N do dia destaca os riscos de executar serviços complexos no espaço do kernel. Enquanto o KSMBD oferece benefícios de desempenho, ele expande a superfície de ataque para execução de código remoto.

Os administradores devem preferir servidores de SMB no espaço do usuário, a menos que o desempenho no nível do kernel seja essencial e garantir o patch em tempo hábil de atualizações de segurança.

Monitoramento contínuo para tráfego incomum de SMB e desativar o acesso anônimo Acesso atenuam ainda mais o risco. A revisão contínua dos módulos do kernel e a implantação cautelosa de novos serviços permanecem críticos para manter a segurança do sistema.

Encontre esta história interessante! Siga -nos LinkedIn**e**X**Para obter mais atualizações instantâneas**.