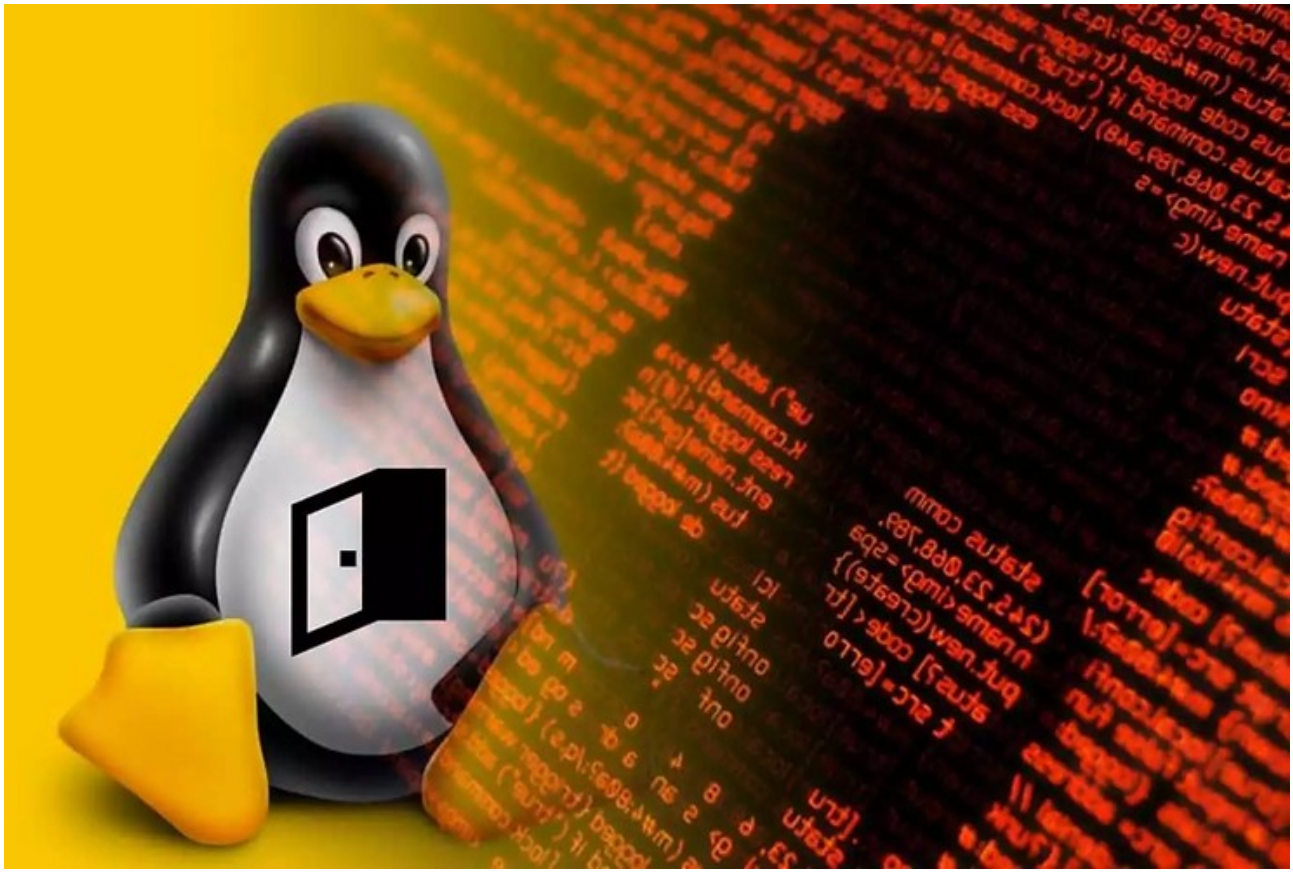
Nova vulnerabilidade no Kernel Linux



No dia 26/12/2022 uma notícia abalou o mundo da segurança cibernética, uma nova vulnerabilidade crítica no kernel do Linux, mais especificamente no módulo do kernel "KSMBD", que implementa o protocolo SMB3 a nível de kernel.

A exploração dessa vulnerabilidade pode permitir a execução de códigos arbitrários por um usuário não autenticado, motivo pelo qual a vulnerabilidade quando identificada, no dia 22/12/2022 como "zero day", recebeu um score 10 na escala de pontuação CVSS, o nível mais alto de criticidade (ZDI-22-1690). Essa nova vulnerabilidade já recebeu 6 CVEs no Mitre, são elas: CVE-2022-47938, CVE-2022-47939, CVE-2022-47940, CVE-2022-47941, CVE-2022-47942 and CVE-2022-47943.

Informações confusas, incompletas e com erros

Apesar de toda a criticidade do assunto, nós encontramos muitas informações confusas, fragmentadas, incompletas e inclusive com erros, em fóruns, artigos e publicações em redes sociais, levando muitas pessoas ou a um desespero desnecessário ou a uma falsa sensação de segurança.

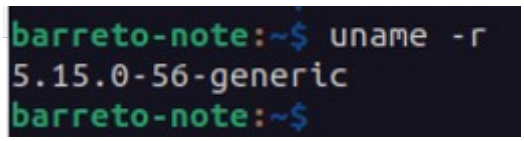
Essas informações divergentes levaram inclusive a criação e divulgação de scripts que prometem analisar se o kernel está vulnerável mas, no entando, o que vimos por aí são, em sua grande maioria, scripts que testam apenas uma parte do ambiente, gerando falsos positvos ou, ainda pior, falsos negativos, piorando ainda mais a confusão sobre o assunto.

Outro ponto percebido foi o entendimento de que o simples fato de atualizar o kernel para uma versão acima da 5.15.x resolveria. No entanto, a vulnerabilidade está presente em muitas releases das versões superiores também, o que tem gerado mais confusão e falsos negativos na análise do ambiente.

Como testar o seu kernel

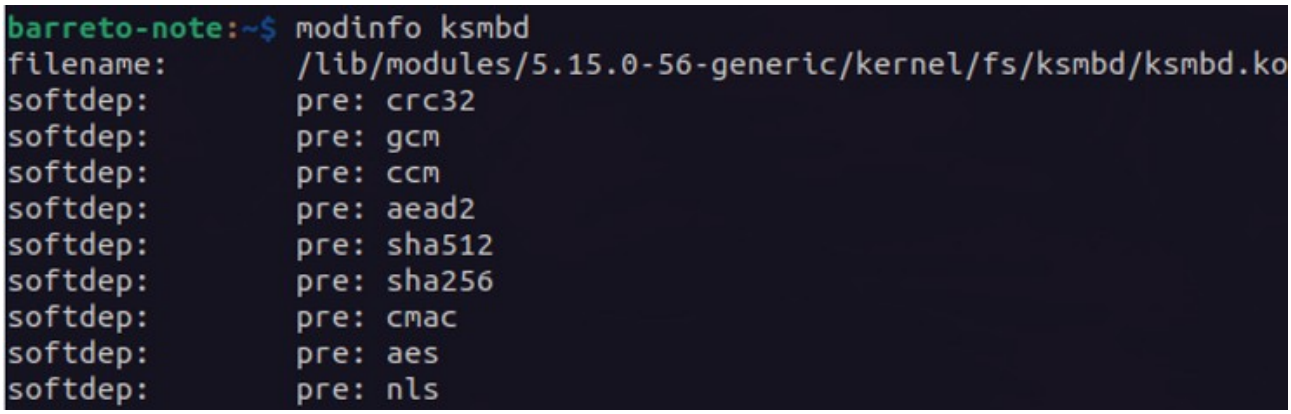
As versões vulneráveis do kernel são 5.15.x (menor que 5.15.61), 5.16.x , 5.17.x, 5.18.x, 5.19.x (menor que 5.19.2).

Para analisar se o seu kernel é potencialmente vulnerável, o primeiro passo é ver se a versão está entre as que contem a vulnerabilidade. Para isso pode-se usar o comando: ***"uname -r"***.



Caso o seu kernel esteja em alguma das versões vulneráveis, o próximo passo é verificar se existe o módulo KSMBD. Para isso pode-se usar o comando: ***"modinfo ksmbd"***.

Se tiver um retorno como o abaixo, então o módulo existe.



Caso o módulo existe é preciso, então, verificar se ele está carregado no kernel, afinal, se o módulo vulnerável for carregado, aquele código com problema não será executado. Para isso pode-se usar o comando: ***"lsmod | grep ksmbd"***.

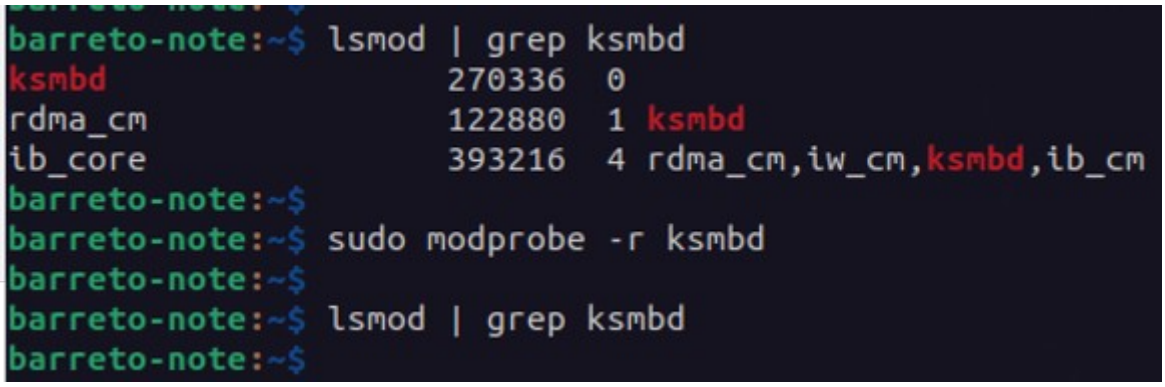
O que fazer se meu Kernel estiver vulnerável?

Uma boa parte das pessoas não vai passar daqui, mas, caso você esteja na minoria que recebeu um retorno como o abaixo, então dispare o alarme!

Nesse ponto você tem 2 opções viáveis:

1) Atualizar o kernel para uma versão contendo a correção para essa vulnerabilidade;

2) Remover o módulo do kernel e, com isso, parar todo e qualquer serviço que use ele, mais especificamente o compartilhamento de arquivos (share) via SMB. Para isso pode-se usar o comando: ***"modprobe -r ksmbd"*** usando "sudo" ou uma conta com privilégios de root



Automatizando o teste da vulnerabilidade

Para facilitar a análise da vulnerabilidade em seu kernel, disponibilizamos um script próprio que pode ser usado para fazer o teste de vulnerabilidade do kernel ao módulo KSMBD.

Você pode acessar o script através do github
https://github.com/andrebarretosantos/security/blob/main/check_ksmbd_kernel_vulnerability.sh

Na linha de comando do seu Linux você pode executar a seguinte sequencia de comandos:
$ wget https://raw.githubusercontent.com/andrebarretosantos/security/main/check_ksmbd_kernel_vulnerability.sh
$ chmod 700 check_ksmbd_kernel_vulnerability.sh
$ ./check_ksmbd_kernel_vulnerability.sh

Recomendações finais

Independentemente do seu Kernel estar vulnerável agora ou não, é recomendado mantê-lo atualizado com os patches de segurança, assim como todo o restante do seu sistema operacional GNU/Linux, afinal, ele está sendo cada vez mais usado e, consequentemente, sendo cada mais visado também.