Linux Kernel 5.8 5.16.11 - Local Privilege Escalation (DirtyPipe)

https://www.exploit-db.com/exploits/50808

Neith Security

Vulnerabilidade DirtyPipe (Linux Kernel 5.8 - 5.16.11)

A vulnerabilidade DirtyPipe é uma falha de escalação de privilégios local que afeta os kernels Linux 5.8 a 5.16.11. Ela permite que um processo não privilegiado sobrescreva arbitrariamente arquivos arbitrários, incluindo arquivos do sistema.

A vulnerabilidade decorre de uma falha na função `pipe2()` do kernel Linux, que é usada para criar pares de pipes. Quando um pipe é criado com os sinalizadores `O_CLOEXEC` e `O_NONBLOCK`, o kernel não define corretamente a permissão de acesso aos arquivos de pipe para o processo filho. Como resultado, um processo filho não privilegiado pode sobrescrever qualquer arquivo no sistema, desde que possa abrir o arquivo para gravação.

Impacto

A vulnerabilidade DirtyPipe pode ser explorada para obter privilégios de root em sistemas Linux afetados. Isso pode levar à execução de código arbitrário, acesso não autorizado a dados confidenciais e comprometimento completo do sistema.

Prevenção

No Windows

Como o Windows não é afetado pela vulnerabilidade DirtyPipe, nenhuma ação específica é necessária para se proteger contra ela no Windows. No entanto, é sempre recomendável manter seu sistema operacional e aplicativos atualizados para se proteger contra outras vulnerabilidades.

No Linux

1. Atualizar o kernel do Linux

A vulnerabilidade DirtyPipe foi corrigida no kernel do Linux 5.16.12. Aplique a atualização mais recente do kernel para se proteger contra a vulnerabilidade.

```
sudo apt update
sudo apt install linux-image-$(uname -r)
sudo reboot
```

2. Remova os patches

Se você aplicou patches ao seu kernel Linux para corrigir a vulnerabilidade DirtyPipe, remova-os após aplicar a atualização do kernel.

```
cd /boot
sudo rm initramfs-linux.img
sudo rm vmlinuz-linux
sudo update-grub
```

3. Limite as permissões de acesso

Você também pode limitar as permissões de acesso aos arquivos de pipe para evitar que sejam sobrescritos.

```
sudo chmod o-w /proc/
sudo chown root:root /proc/
```

4. Use SELinux

O SELinux (Security-Enhanced Linux) é um módulo de segurança do kernel que pode ser usado para restringir o acesso a arquivos e recursos do sistema. Habilite o SELinux no seu sistema Linux para adicionar uma camada extra de proteção.

```
sudo setenforce 1
```

5. Monitore atividades suspeitas

Monitore as atividades do sistema em busca de processos ou comandos suspeitos que possam estar explorando a vulnerabilidade DirtyPipe.

```
sudo auditctl -w /proc/ -p wa -k dirtypipe
```

Conclusão

A vulnerabilidade DirtyPipe representa um risco significativo para sistemas Linux afetados. Aplique as medidas de prevenção acima para se proteger contra a exploração desta vulnerabilidade e manter seus sistemas Linux seguros.