Linux Kernel 5.8 5.16.11 - Local Privilege Escalation (DirtyPipe)

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

O que é Linux Kernel 5.8 - 5.16.11 - Local Privilege Escalation (DirtyPipe)?

O Linux Kernel 5.8 - 5.16.11 - Local Privilege Escalation (DirtyPipe) é uma vulnerabilidade de escalonamento de privilégios locais que afeta sistemas Linux que usam o protocolo de pipe nomeado. A vulnerabilidade permite que um usuário não privilegiado obtenha privilégios de root no sistema alvo.

A vulnerabilidade existe devido a uma falha no subsistema de pipe nomeado do kernel Linux. Quando um usuário cria um pipe nomeado, o kernel aloca um buffer de memória para armazenar os dados escritos no pipe. No entanto, a vulnerabilidade DirtyPipe permite que um usuário sobrescreva o conteúdo do buffer de memória do pipe nomeado com dados arbitrários. Isso pode levar ao escalonamento de privilégios, pois permite que o usuário modifique dados confidenciais do sistema ou execute código malicioso com privilégios de root.

Como se proteger do DirtyPipe?

Existem várias medidas que você pode tomar para se proteger do DirtyPipe:

- Aplique patches: A Red Hat, Debian e outras distribuições Linux lançaram patches para corrigir a vulnerabilidade DirtyPipe. Aplique esses patches em seus sistemas o mais rápido possível.

Comandos para ambientes Linux:

-`sudo yum update` ou `sudo apt update` (para atualizar o sistema)

-`sudo reboot` (para reiniciar o sistema após a atualização)

Comandos para ambientes Windows:

-Não há comandos específicos para proteger sistemas Windows do DirtyPipe, pois a vulnerabilidade afeta apenas sistemas Linux.

Outras medidas de mitigação:

- Use SELinux ou AppArmor: Esses módulos de segurança podem ajudar a restringir as ações que processos não privilegiados podem executar e podem fornecer proteção adicional contra exploits DirtyPipe.

- Desabilitar pipes nomeados desnecessários: Se você não estiver usando pipes nomeados, considere desabilitá-los em todo o sistema ou desabilitar pipes específicos que não estão sendo usados.

- Monitore seu sistema: Monitore seus logs do sistema e arquivos de auditoria para detectar quaisquer atividades suspeitas que possam indicar um exploit DirtyPipe.

Recomendações adicionais:

-Mantenha seu sistema atualizado com os patches de segurança mais recentes.

-Use software antivírus e antimalware para detectar e bloquear malware que pode explorar o DirtyPipe.

-Faça backup regular de seus dados importantes para que você possa restaurá-los no caso de um ataque.

O DirtyPipe é uma vulnerabilidade séria que pode permitir que invasores obtenham acesso não autorizado a sistemas Linux. É crucial tomar medidas para corrigir esta vulnerabilidade o mais rápido possível. Seguindo estas recomendações, você pode ajudar a proteger seu sistema contra

ataques do DirtyPipe.

ProFTPd 1.3.5 - mod_copy Remote Command Execution (2)

https://www.exploit-db.com/exploits/49908

ProFTPD 1.3.5 - mod_copy Execução Remota de Comando (2): Visão Geral

O ProFTPD é um servidor FTP de código aberto amplamente usado que oferece recursos de transferência de arquivos segura e confiável. No entanto, uma vulnerabilidade crítica de execução remota de código (RCE) foi descoberta na versão 1.3.5 do ProFTPD, especificamente no módulo mod_copy.

Esta vulnerabilidade permite que um invasor envie um comando especialmente criado para o servidor ProFTPD, o que pode levar à execução arbitrária de código no sistema subjacente. Isso pode dar ao invasor controle total sobre o servidor, incluindo a capacidade de modificar, excluir ou ler arquivos, instalar malware ou comprometer outros sistemas na rede.

Protegendo-se da Vulnerabilidade

Para se proteger desta vulnerabilidade, é crucial atualizar o ProFTPD para a versão mais recente (atualmente 1.3.6) o mais rápido possível. A nova versão aborda a vulnerabilidade e impede que ela seja explorada.

Comandos para Atualizar o ProFTPD em Ambientes Linux e Windows

Linux:

- `sudo apt-get update && sudo apt-get install proftpd`

Windows:

- Baixe o instalador do ProFTPD do site oficial.

- Execute o instalador e siga as instruções na tela.

- Certifique-se de selecionar a opção "Atualizar" se o ProFTPD já estiver instalado.

Comandos Adicionais para Verificar a Versão do ProFTPD

Linux:

- `dpkg --list | grep proftpd`

Windows:

- Execute "proftpd -version" no prompt de linha de comando.

Outras Medidas de Proteção

Além da atualização, existem outras medidas de proteção que podem ser implementadas para reduzir ainda mais o risco:

- Use um Firewall: Implemente um firewall para bloquear o acesso ao servidor FTP de IPs não autorizados.

- Limite o Acesso: Conceda acesso ao servidor FTP apenas aos usuários que precisam dele.

- Monitore Logs do Servidor: Monitore regularmente os logs do servidor para identificar qualquer atividade suspeita.

- Mantenha o Software Atualizado: Mantenha o sistema operacional e todos os softwares instalados atualizados com os patches de segurança mais recentes.

Conclusão

A vulnerabilidade ProFTPD 1.3.5 - mod_copy RCE é uma ameaça séria que pode comprometer os servidores FTP e os sistemas subjacentes. Ao atualizar para a versão mais recente do ProFTPD e implementar medidas adicionais de proteção, as organizações podem proteger seus sistemas e dados contra essa vulnerabilidade crítica.