Neith Security

2024

Relatório Neith

Your Future is Secure

Presented By: Carlos Henrique

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 contém uma vulnerabilidade de escalação de privilégios locais (CVE-2022-0847) conhecida como "DirtyPipe". Esta vulnerabilidade permite que um usuário não privilegiado obtenha privilégios de root no sistema.

Como a vulnerabilidade DirtyPipe funciona

O pipe nomeado é um recurso do sistema Linux que permite que os processos se comuniquem por meio de arquivos. Um pipe nomeado cria uma conexão bidirecional entre dois processos, permitindo que eles leiam e escrevam dados um ao outro.

A vulnerabilidade DirtyPipe ocorre em um trecho de código que lida com pipes nomeados. Quando um processo grava em um pipe nomeado, os dados são armazenados em buffer até que possam ser lidos pelo processo receptor. A vulnerabilidade DirtyPipe permite que um processo leia dados de um buffer de pipe nomeado antes que ele tenha sido totalmente sobrescrito pelo processo de gravação.

Isso pode levar à escalação de privilégios porque o processo de leitura pode ser capaz de ler dados confidenciais, como senhas ou tokens de autenticação, que foram armazenados no buffer de pipe nomeado por outro processo com privilégios mais altos.

Como se proteger da vulnerabilidade DirtyPipe

A maneira mais eficaz de se proteger da vulnerabilidade DirtyPipe é atualizar seu kernel Linux para uma versão que tenha o patch para a vulnerabilidade. As versões do kernel com o patch são:

-Linux Kernel 5.8.20

-Linux Kernel 5.9.18

-Linux Kernel 5.10.102

-Linux Kernel 5.11.21

-Linux Kernel 5.12.14

-Linux Kernel 5.13.12

-Linux Kernel 5.14.16

-Linux Kernel 5.15.25

-Linux Kernel 5.16.13

Para atualizar seu kernel Linux, execute os seguintes comandos:

Para distribuições Debian/Ubuntu:

```
sudo apt update
sudo apt upgrade
```

Para distribuições Red Hat/CentOS:

```
sudo yum update kernel
sudo reboot
```

Além de atualizar o kernel, você também pode proteger seu sistema contra a vulnerabilidade DirtyPipe desabilitando os pipes nomeados. No entanto, isso pode afetar a funcionalidade de alguns programas que dependem de pipes nomeados. Para desabilitar os pipes nomeados, execute os seguintes comandos:

Para distribuições Debian/Ubuntu:

```
sudo sysctl -w fs.pipe-buffer-size=0
```

Para distribuições Red Hat/CentOS:

```
sudo sysctl -w fs.pipe-buffer-size=0
```

Como se proteger da vulnerabilidade DirtyPipe em ambientes Windows

O Windows não é afetado diretamente pela vulnerabilidade DirtyPipe. No entanto, os sistemas Windows podem ser afetados se estiverem compartilhando arquivos com sistemas Linux que são vulneráveis à vulnerabilidade DirtyPipe.

Para proteger seu sistema Windows da vulnerabilidade DirtyPipe, você deve:

-Atualize o kernel Linux em qualquer sistema Linux que esteja compartilhando arquivos com seu sistema Windows.

-Desabilite ou restrinja o compartilhamento de arquivos entre sistemas Linux e Windows.

-Implemente medidas de segurança adicionais, como firewalls e sistemas de detecção de intrusão, para proteger seu sistema Windows contra acesso não autorizado.

ProFTPd - mod_sftp Integer Overflow Denial of Service (PoC)

https://www.exploit-db.com/exploits/16129

ProFTPd - mod_sftp Integer Overflow Denial of Service (PoC)

O ProFTPd é um servidor FTP altamente seguro e flexível que suporta vários protocolos, incluindo SFTP (SSH File Transfer Protocol). A vulnerabilidade mod_sftp Integer Overflow no ProFTPd permite que os invasores causem uma negação de serviço (DoS) enviando uma sequência de pacotes SFTP especificamente projetada.

Como Funciona a Vulnerabilidade

A vulnerabilidade decorre de um estouro de inteiro no código que processa pacotes SFTP no modulo mod_sftp do ProFTPd. Mais especificamente, um campo de comprimento de pacote não verificado pode ser manipulado para exceder o tamanho máximo esperado, resultando em um estouro de buffer e um travamento do servidor.

Impacto da Vulnerabilidade

Se explorada com sucesso, essa vulnerabilidade pode levar a uma negação de serviço, impedindo os usuários de acessar o servidor FTP. Os invasores poderiam usar essa vulnerabilidade para interromper o acesso a arquivos críticos ou para lançar ataques de amplificação de negação de serviço (DoS), onde os pacotes maliciosos são amplificados e direcionados a um alvo para sobrecarregá-lo.

Como se Proteger

Ambientes Linux

1. Atualize o ProFTPd:

- `yum upgrade proftpd` (para sistemas baseados em RPM)
- `apt-get update && apt-get upgrade proftpd` (para sistemas baseados em Debian)

2. Reconfigure o ProFTPd:

- Edite o arquivo de configuração do ProFTPd (`/etc/proftpd.conf`):
- Adicione ou altere a seguinte linha: `SFTPOptions RequireValidSize`
- Salve e reinicie o ProFTPd: `systemctl restart proftpd.service`

Ambientes Windows

O ProFTPd não é amplamente usado em ambientes Windows. No entanto, se você estiver usando o ProFTPd no Windows, siga estas etapas:

1. Atualize o ProFTPd:

- Baixe e instale a versão mais recente do ProFTPd no site oficial.

2. Reconfigure o ProFTPd:

- Abra o "Gerenciador do Servidor FTP" e navegue até a guia "Configurações".
- Em "Configurações avançadas", adicione ou altere a seguinte linha: `SFTPOptions RequireValidSize`
- Salve e reinicie o ProFTPd.

Medidas Adicionais de Proteção

Além de corrigir a vulnerabilidade, as seguintes medidas adicionais podem ajudar a proteger seu servidor:

- Use um firewall:

- Configure um firewall para bloquear conexões não autorizadas ao servidor FTP.

- Limite as conexões:

- Configure o ProFTPd para limitar o número de conexões simultâneas.

- Monitore o servidor:

- Monitore os logs do servidor e o tráfego de rede para identificar quaisquer atividades suspeitas.

- Faça backups regulares:

- Faça backups regulares dos dados importantes em seu servidor FTP para evitar perda de dados em caso de um ataque.

Conclusão

A vulnerabilidade ProFTPd - mod_sftp Integer Overflow Denial of Service é uma falha séria que pode ser explorada por invasores para causar negação de serviço. Ao aplicar o patch e implementar medidas adicionais de proteção, você pode reduzir significativamente o risco de exploração e proteger seu servidor FTP.

Apache Httpd mod_rewrite - Open Redirects

https://www.exploit-db.com/exploits/47689

Introdução ao Apache Httpd mod_rewrite - Open Redirects

O Apache Httpd mod_rewrite é um módulo de reescrita de URL que permite aos administradores de sites redirecionar, regravar ou reescrever solicitações HTTP com base em regras definidas. Ele é amplamente usado para fins administrativos, como redirecionamentos 301 para URLs antigas ou novas, remoção de parâmetros de consulta ou reescrita de padrões de URL complexos para simplificá-los.

Open Redirects

Um Open Redirect é uma vulnerabilidade que permite que um invasor redirecionamento os usuários para um site malicioso de sua escolha. Isso ocorre quando um aplicativo da Web aceita um parâmetro de consulta não confiável que contém um URL e o redireciona para esse URL sem verificar sua legitimidade.

No Apache Httpd com mod_rewrite, os Open Redirects podem ser criados quando as regras de reescrita usam expressões regulares que não validam adequadamente a entrada do usuário. Por exemplo, a seguinte regra de reescrita é vulnerável a Open Redirects:

```
RewriteRule ^redirect/(.*)$ https://attacker-controlled-domain.com/$1 [R]
```

Esta regra redireciona todas as solicitações para `/redirect/` para um domínio controlado pelo invasor especificado no parâmetro de consulta. Um invasor pode explorar essa vulnerabilidade criando um link para um site legítimo com um parâmetro de consulta apontando para seu próprio domínio malicioso, como:

```

https://legitimate-site.com/redirect/?url=https://attacker-controlled-domain.com/

```

Proteção Contra Open Redirects

Existem várias medidas que podem ser tomadas para proteger contra Open Redirects no Apache Httpd com mod_rewrite:

- Valide a Entrada do Usuário: As expressões regulares das regras de reescrita devem ser escritas com cuidado para garantir que elas validem adequadamente a entrada do usuário. Por exemplo, a expressão regular usada acima poderia ser aprimorada para validar URLs:

```

RewriteRule ^redirect/(.*)$ https:///((?!attacker-controlled-domain.com).)*$ [R]

```

- Use o sinalizador `[L]`: O sinalizador `[L]` nas regras de reescrita interrompe o processamento de mais regras se a regra corresponder. Isso pode ajudar a prevenir que um Open Redirect seja redirecionado para uma segunda vulnerabilidade.

- Use o sinalizador `[F]`: O sinalizador `[F]` nas regras de reescrita faz com que o Apache verifique se o destino do redirecionamento existe antes de redirecioná-lo. Isso pode ajudar a prevenir a exploração de Open Redirects.

- Use o módulo `mod_setenvifnocase`: O módulo `mod_setenvifnocase` pode ser usado para definir variáveis de ambiente com base em cabeçalhos de solicitação. Isso pode ser usado para rastrear tentativas de redirecionamento e bloquear solicitações com URLs suspeitos.

Comandos para Proteção Contra Open Redirects

Linux

Os seguintes comandos podem ser usados para proteger contra Open Redirects no Apache Httpd em sistemas Linux:

```
# Verifique se o mod_rewrite está carregado
apachectl -t -D DUMP_MODULES | grep rewrite
# Adicione as seguintes linhas ao seu arquivo de configuração do Apache Httpd:
<IfModule mod_rewrite.c>
  RewriteEngine On
  RewriteRule ^redirect/(.*)$ https://((?!attacker-controlled-domain.com).)*$ [R,L]
  RewriteCond %{HTTP:Referer} ^https?://(www\.)?attacker-controlled-domain\.com [NC]
  RewriteRule ^redirect/(.*)$ https://www.legitimate-site.com/ [R,L]
</IfModule>
# Reinicie o Apache Httpd
service apache2 restart
```

Windows

Os seguintes comandos podem ser usados para proteger contra Open Redirects no Apache Httpd em sistemas Windows:

-Abra o Gerenciador do Apache HTTP Server.

-Clique em "Configuração" no menu Iniciar.

-Na seção "Tipos de módulo", clique em "Configuração" ao lado de "mod_rewrite".

-Adicione as seguintes linhas ao arquivo de configuração:

```
RewriteEngine On
RewriteRule ^redirect/(.*)$ https://((?!attacker-controlled-domain.com).)*$ [R,L]
RewriteCond %{HTTP:Referer} ^https?://(www\.)?attacker-controlled-domain\.com [NC]
RewriteRule ^redirect/(.*)$ https://www.legitimate-site.com/ [R,L]
```

-Clique em "Salvar" e reinicie o Apache Httpd.

Conclusão

Os Open Redirects são vulnerabilidades graves que podem permitir que os invasores redirecionamento os usuários para sites maliciosos. Ao seguir as práticas recomendadas de segurança, como validar a entrada do usuário, usar sinalizadores apropriados e potencialmente usar módulos adicionais, os administradores podem proteger seus sites Apache Httpd mod_rewrite contra essa vulnerabilidade.

ProFTPd 1.3.5 - mod_copy Remote Command Execution (2)

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

Vulnerabilidade ProFTPd 1.3.5 - mod_copy Remote Command Execution (2)

O ProFTPd é um servidor FTP amplamente utilizado que apresentava uma vulnerabilidade de execução remota de comando (RCE) crítica no módulo mod_copy. Isso permitia que um invasor não autenticado executasse comandos arbitrários no servidor.

Como Explorar:

Um invasor poderia explorar esta vulnerabilidade enviando uma solicitação FTP especialmente elaborada para o servidor ProFTPd. A solicitação continha um comando "COPY" malicioso que executava um shell no servidor. O invasor então poderia usar o shell para controlar remotamente o sistema.

Impacto:

Esta vulnerabilidade permitia que um invasor obtivesse acesso total ao servidor FTP comprometido, incluindo a capacidade de:

-Executar comandos no servidor

-Ler e escrever arquivos

-Modificar ou excluir configurações

-Instalar ou remover software

-Baixar ou carregar dados confidenciais

Ambientes Vulneráveis:

Esta vulnerabilidade afetava sistemas que executavam ProFTPd versões 1.3.5 e anteriores com o módulo mod_copy ativado.

Como se Proteger

Ambientes Linux:

1. Atualize o ProFTPd: Aplique o patch de segurança mais recente, que aborda esta vulnerabilidade.

2. Desative o módulo mod_copy:

```bash
nano /etc/proftpd.conf
```

Adicione a seguinte linha ao final do arquivo:

```conf
Module off mod_copy
```

Salve e saia do arquivo.

3. Reinicie o ProFTPd:

```bash
sudo service proftpd restart
```

Ambientes Windows:

1. Atualize o ProFTPd: Baixe e instale a versão mais recente do ProFTPd do site oficial.

2. Desative o módulo mod_copy: Edite o arquivo "proftpd.conf" localizado no diretório de instalação do ProFTPd e adicione a seguinte linha ao final do arquivo:

```conf
Module off mod_copy
```

Salve e saia do arquivo.

3. Reinicie o ProFTPd: Use o Prompt de Comando do Windows para executar o seguinte comando:

```cmd
net stop "ProFTPD Service" && net start "ProFTPD Service"
```

Recomenda-se também tomar as seguintes medidas de segurança adicionais:

-Habilite um firewall para bloquear o acesso não autorizado ao servidor FTP.

-Use chaves SSH para autenticação segura.

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

-Monitorize regularmente seu servidor em busca de atividades suspeitas.

-Faça backups regulares de seus dados.

Neith Security

Your future is secure

Neith Security