Neith Security

2024

Relatório Neith

Your Future is Secure

Presented By: Carlos Henrique

Apache Httpd mod_rewrite - Open Redirects

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

Neith Security

Vulnerabilidade Open Redirects

Open Redirects é uma vulnerabilidade de segurança que permite que um invasor redirecionamentos os usuários para sites mal-intencionados. Ela ocorre quando um aplicativo da web aceita parâmetros de URL que redirecionam os usuários sem validar adequadamente esses parâmetros.

Como funciona no Apache Httpd mod_rewrite

O Apache Httpd mod_rewrite é um módulo do servidor web Apache HTTP que permite que os administradores de sites reescrevam ou modifiquem solicitações de URL. Isso é útil para criar redirecionamentos, ocultar a estrutura do URL ou alterar o comportamento do servidor com base nos parâmetros da URL.

A vulnerabilidade Open Redirect no mod_rewrite ocorre quando um invasor insere parâmetros maliciosos em uma solicitação de URL que redireciona os usuários para um site controlado pelo invasor. Isso pode ser feito adicionando o parâmetro `[R=302]` a uma solicitação de URL, que instrui o servidor a redirecionar o usuário com um código de status HTTP 302.

Prevenindo Open Redirects no Windows

No Windows, você pode usar o recurso de proteção contra redirecionamento externo no IIS (Internet Information Services) para evitar Open Redirects. Para ativar esse recurso:

1. Abra o Gerenciador do IIS.
2. Selecione o site que deseja proteger.

3. No painel Ações, clique em "Configurar redirecionamento externo".

4. Na caixa de diálogo "Proteção contra redirecionamento externo", marque a opção "Bloquear todos os redirecionamentos externos" e clique em "OK".

Prevenindo Open Redirects no Linux

No Linux, existem várias maneiras de prevenir Open Redirects no Apache Httpd mod_rewrite:

- Use expressões regulares para validar parâmetros: Use expressões regulares para garantir que os parâmetros de URL contenham apenas caracteres válidos e não permitam caracteres que possam ser usados para criar redirecionamentos maliciosos.

- Verifique a lista de permissões de domínios permitidos: Crie uma lista de permissões de domínios permitidos que o servidor pode redirecionar e bloqueie todos os outros.

- Use mod_headers: Use o módulo mod_headers do Apache para definir cabeçalhos de resposta HTTP que impeçam o navegador de seguir redirecionamentos externos.

Comandos de exemplo

Windows (IIS)

```
<configuration>
    <system.webServer>
```

```
        <security>
            <requestFiltering>
                <denyUrlPathTokens>
                    <add token="[R=302]" />
                </denyUrlPathTokens>
            </requestFiltering>
        </security>
    </system.webServer>
</configuration>
```

Linux (Apache Httpd)

```
RewriteEngine On
RewriteCond %{REQUEST_URI} ^/redirect/(.*)$
RewriteCond %{REQUEST_METHOD} GET
RewriteCond %{QUERY_STRING} ^.+=http://(.*)$
RewriteRule ^.*$ http://%1 [R=403,L]
```

Este comando reescreverá todas as solicitações de URL que comecem com "/redirect/" e contenham um parâmetro de consulta que especifique um URL externo para o domínio autorizado "%1". Se a condição for atendida, a solicitação será bloqueada com um código de status HTTP 403 (Proibido).


Neith
Security

Linux Kernel 5.8 5.16.11 - Local Privilege Escalation (DirtyPipe)

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

Neith Security

Vulnerabilidade Local Privilege Escalation (Dirty Pipe)

O Local Privilege Escalation (LPE), conhecido como Dirty Pipe, é uma vulnerabilidade crítica no kernel do Linux que permite que um atacante não privilegiado aumente seus privilégios para root e obtenha acesso total ao sistema.

Como funciona o Dirty Pipe

O Dirty Pipe explora uma vulnerabilidade na forma como o kernel do Linux lida com arquivos de mapeamento de memória (MMAP). O MMAP permite que os aplicativos acessem arquivos diretamente na memória, sem copiar os dados para o espaço do usuário. Isso pode melhorar o desempenho, mas também pode introduzir vulnerabilidades de segurança.

No caso do Dirty Pipe, um atacante pode escrever dados arbitrários nos arquivos de mapeamento de memória de processos privilegiados, como o daemon SSH. Isso permite que o atacante altere as permissões de arquivos críticos ou execute comandos arbitrários como root.

Como se proteger do Dirty Pipe no Windows

Como o Dirty Pipe é uma vulnerabilidade do Linux, não afeta diretamente os sistemas Windows. No entanto, se um sistema Windows estiver conectado a um servidor Linux vulnerável, o atacante pode explorar a vulnerabilidade para obter acesso ao sistema Windows.

Para se proteger, os usuários do Windows devem garantir que seus sistemas estejam atualizados com os patches de segurança mais recentes. Eles também devem ter cuidado ao estabelecer conexões com servidores Linux desconhecidos ou não confiáveis.

Neith Security

Como se proteger do Dirty Pipe no Linux

Para se proteger do Dirty Pipe no Linux, os usuários devem seguir estas etapas:

1. Aplique as atualizações de segurança: A versão mais recente do kernel do Linux (5.16.11) corrige a vulnerabilidade do Dirty Pipe. Os usuários devem atualizar seus sistemas para esta versão ou versões posteriores o mais rápido possível.

2. Use RPM ou DEB: Instale o pacote de correção RPM ou DEB (para distribuições baseadas em Red Hat ou Debian, respectivamente) fornecido pelo seu fornecedor.

3. Compile o kernel personalizado: Compilar o kernel personalizado com a correção do Dirty Pipe aplicada. Consulte a documentação do kernel do Linux para obter instruções.

Comandos Linux para aplicar as atualizações

Para aplicar as atualizações de segurança no Linux, use os seguintes comandos:

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

Para verificar se o kernel foi atualizado, execute o seguinte comando:

```
uname -r
```

```

Ele deve exibir a versão do kernel 5.16.11 ou superior.

**Conclusão**

A vulnerabilidade do Dirty Pipe é uma séria ameaça de segurança que pode permitir que atacantes obtenham acesso root em sistemas Linux. É essencial aplicar as atualizações de segurança mais recentes e tomar as precauções adequadas para proteger seus sistemas 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)

A vulnerabilidade ProFTPd 1.3.5 - mod_copy Remote Command Execution (2) permite que um invasor remoto execute comandos arbitrários no sistema host executando o servidor ProFTPd. Isso pode levar à execução de código, acesso a dados confidenciais ou outras ações maliciosas.

A vulnerabilidade existe devido a uma falha de verificação de entrada no módulo mod_copy do ProFTPd 1.3.5. Essa falha permite que um invasor forneça um nome de arquivo especialmente criado que contém comandos arbitrários. Quando o nome do arquivo é processado pelo módulo mod_copy, os comandos são executados no sistema host.

Como se proteger no Windows

Para se proteger contra esta vulnerabilidade no Windows, é recomendável aplicar a atualização de segurança mais recente da Microsoft que aborda este problema. A atualização está disponível para download no site da Microsoft.

Além disso, as seguintes etapas adicionais podem ser tomadas para fortalecer a segurança:

- Desative o módulo mod_copy se não for necessário.
- Use um firewall para restringir o acesso ao servidor ProFTPd apenas de hosts confiáveis.
- Habilite o recurso "Permitir Somente Usuários Específicos" no ProFTPd para restringir o acesso ao servidor a usuários específicos.
- Use um scanner de vulnerabilidade para verificar regularmente se há vulnerabilidades e corrija-as o mais rápido possível.

Como se proteger no Linux

Para se proteger contra esta vulnerabilidade no Linux, é recomendável aplicar a atualização de segurança mais recente do seu fornecedor de distribuição. A atualização está disponível para download no site do fornecedor da distribuição.

Além disso, as seguintes etapas adicionais podem ser tomadas para fortalecer a segurança:

- Desative o módulo mod_copy se não for necessário.
- Use um firewall para restringir o acesso ao servidor ProFTPd apenas de hosts confiáveis.
- Habilite o recurso "Permitir Somente Usuários Específicos" no ProFTPd para restringir o acesso ao servidor a usuários específicos.
- Adicione as seguintes linhas ao arquivo de configuração do ProFTPd (/etc/proftpd.conf):

```
DenyConnect \- .localdomain
AllowConnect \*
```

Isso negará as conexões de hosts com o domínio ".localdomain" e permitirá conexões de todos os outros hosts.

- Use um scanner de vulnerabilidade para verificar regularmente se há vulnerabilidades e corrija-as o mais rápido possível.

Comandos para se proteger

Windows

```
wusa.exe /install:path\to\update.msu
```

```

**Linux**

```

apt-get update && apt-get upgrade

```

```

yum update

```

```

dnf update

```

**Conclusão**

A vulnerabilidade ProFTPd 1.3.5 - mod_copy Remote Command Execution (2) representa um risco significativo à segurança para sistemas que executam o servidor ProFTPd. É crucial aplicar as atualizações de segurança mais recentes e tomar medidas adicionais para fortalecer a segurança, conforme descrito neste documento. Ao seguir estas recomendações, você pode mitigar o risco de exploração desta vulnerabilidade e proteger seus sistemas contra ataques maliciosos.
```

ProFTPd - mod_sftp Integer Overflow Denial of Service (PoC)

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

Neith Security

Vulnerabilidade ProFTPd - mod_sftp Integer Overflow Denial of Service (PoC)

O ProFTPd é um servidor FTP gratuito e de código aberto amplamente utilizado que fornece acesso a arquivos em sistemas Linux e Windows. O módulo mod_sftp do ProFTPd permite que os usuários acessem arquivos remotamente por meio do protocolo SSH File Transfer Protocol (SFTP).

Uma vulnerabilidade de estouro de inteiro foi descoberta no módulo mod_sftp do ProFTPd, permitindo que um invasor remoto negasse o serviço (DoS) ao servidor ProFTPd. O estouro de inteiro ocorre quando um aplicativo tenta armazenar um valor numérico que excede a capacidade do tipo de dados alocado. Isso pode levar a comportamentos inesperados e travamentos do aplicativo.

Na vulnerabilidade do ProFTPd mod_sftp, o estouro de inteiro ocorre durante o processamento de pacotes SFTP grandes. Um invasor pode enviar um pacote SFTP especialmente projetado que contenha um valor inválido para o campo "tamanho do pacote". Isso fará com que o módulo mod_sftp do ProFTPd aloque uma quantidade excessiva de memória, resultando em um estouro de inteiro e travamento do servidor.

Prevenção no Windows

Para se proteger contra esta vulnerabilidade no Windows, os usuários podem seguir estas etapas:

1. Aplique o patch mais recente: A Microsoft lançou um patch de segurança que corrige esta vulnerabilidade. Instale o patch o mais rápido possível.

2. Bloqueie a porta 22: O SFTP usa a porta 22 por padrão. Bloqueie esta porta usando um firewall para impedir que invasores acessem o servidor ProFTPd.

---

3. Use um servidor FTP alternativo: Considere usar um servidor FTP alternativo que não seja afetado por esta vulnerabilidade, como o FileZilla Server.

Prevenção no Linux

Para se proteger contra esta vulnerabilidade no Linux, os usuários podem seguir estas etapas:

1. Aplique o patch mais recente: Verifique os repositórios de software da sua distribuição Linux para o patch mais recente e instale-o.

2. Bloqueie a porta 22: Use o comando iptables para bloquear o tráfego na porta 22:

```
sudo iptables -A INPUT -p tcp --dport 22 -j DROP
```

3. Configure o limite de comprimento do pacote: Defina um limite para o comprimento do pacote que o módulo mod_sftp pode aceitar. Isso pode ser feito editando o arquivo de configuração do ProFTPd (/etc/proftpd.conf) e adicionando a seguinte linha:

```
LimitSftpPacketLength 10000
```

Isso limita o comprimento do pacote SFTP para 10.000 bytes.

4. Use um servidor FTP alternativo: Como no Windows, considere usar um servidor FTP alternativo, como o PureFTPd, que não seja afetado por esta vulnerabilidade.

Conclusão

A vulnerabilidade ProFTPd - mod_sftp Integer Overflow Denial of Service é uma ameaça séria que pode permitir que invasores neguem o acesso a arquivos remotos. Ao aplicar os patches e medidas de mitigação descritos acima, os usuários podem proteger seus servidores contra esta vulnerabilidade e garantir a disponibilidade e segurança dos dados.

Neith Security

Your future is secure

Neith Security