

Misceláneo

Capítulo destinado a la solución, mitigación de software en general.

- Mitigar enumeración de usuarios OpenSSH
- Mitigar HeartBleed en OpenSSL

Mitigar enumeración de usuarios OpenSSH

Utilizar versiones antiguas de openssh puede permitir la enumeración de usuarios en SSH, por lo cual es recomendable utilizar versiones posteriores a la 7.7 de OPENSSH, a continuación se detallará de cómo realizar la actualización mediante uso de repositorios.

La presente guía fue probada en un servidor Debian 9.7 con versión 7.4 de OpenSSH.

Visualizar la versión de OpenSSH utilizada:

```
$ sshd -V
```

Agregar el repositorio para la última version de openssh:

```
$ nano /etc/apt/source.list
```

Agregar al final:

```
deb http://ftp.de.debian.org/debian sid main
```

Actualizar la lista de paquetes:

```
$ apt update
```

Instalar OpenSSH:

```
$ apt install openssh-server
```

elegir opcion 1 (install the package maintainer's version)

Verificar la versión instalada:

```
$ telnet localhost 22
```

```
SSH-2.0-OpenSSH_8.4p1 Debian-4
```

Si desea puede comentar le repositorio agregado en source.list

```
$ nano /etc/apt/source.list
```

Colocar # al comienzo de la línea añadida:

```
# deb http://ftp.de.debian.org/debian sid main
```

Actualizar la lista de paquetes:

```
$ apt update
```

Mitigar HeartBleed en OpenSSL

La vulnerabilidad de OpenSSL desactualizado puede permitir a un atacante realizar una variedad de ataques, incluyendo la interceptación de datos cifrados y la inyección de código malicioso. Esta vulnerabilidad puede ser explotada por los atacantes mediante la explotación de una variedad de vulnerabilidades de seguridad conocidas en versiones antiguas de OpenSSL.

Para evitar esta vulnerabilidad, es importante que los sistemas se mantengan actualizados con las últimas versiones de OpenSSL y otros software críticos. También es recomendable realizar auditorías periódicas de seguridad en los sistemas para identificar cualquier vulnerabilidad que pueda estar presente. Además, se deben aplicar medidas de seguridad adicionales, como la utilización de certificados SSL/TLS seguros y la implementación de políticas de autenticación adecuadas, para minimizar el riesgo de ataques.

Actualización OpenSSL en Ubuntu

Esta guía fue probada en un servidor Ubuntu con una versión inicial de OpenSSL de 0.9.8.

Ejecutar el siguiente comando para ver la versión actual de openssl:

```
$ openssl version
```

Y como respuesta nos da la versión y el año de creación del OpenSSL:

```
OpenSSL 0.9.8k 25 mar 2009
```

Descargar desde el repositorio de openssl el archivo al que se actualizará en este caso OpenSSL 1.1.1j:

```
$ https://www.openssl.org/source/openssl-1.1.1j.tar.gz
```

Desempaquetar:

```
$ tar -xzf openssl-1.1.1j.tar.gz
```

Emitir los siguientes comandos para la instalación:

```
$ ./config  
$ make // (si el comando make no está instalado ejecutar $ sudo apt install make gcc)  
$ make install
```

Creando un enlace desde el binario recién instalado a la ubicación predeterminada:

```
$ sudo ln -s /usr/local/bin/openssl /usr/bin/openssl  
$ sudo ldconfig  
$ openssl version
```

La respuesta debe ser parecida a la siguiente:

```
OpenSSL 1.1.1j 16 Feb 2021
```