Bisoños Usuarios de GNU/Linux de Mallorca y Alrededores | Bergantells Usuaris de GNU/Linux de Mallorca i Afegitons

Descubierto fallo de seguridad en el servidor X de Solaris (7461 lectures)

Per **Eduard Llull**, ***Daneel*** ()

Creado el 16/04/2001 20:06 modificado el 16/04/2001 20:06

Recientemente eEye Digital Security[1] ha descubierto un buffer overflow en Xsun, el servidor de X Windows usado en Solaris que puede ser aprovechado para obtener privilegios de root.

En eEye Digital Security[1] podemos leer la noticia[2] del descubrimiento de un buffer overflow en el servidor de X Windows de Solaris, Xsun. Como el servidor está SUID root, se puede aprovechar el buffer overflow para obtener provilegios de root.
Los sistemas vulnerables son Solaris 7/8 (sobre arquitectura x86 y Sparc) y el fallo se fundamenta en la manera en que Xsun maneja la variable de entorno HOME.

```
bash-2.03$ HOME=`perl -e 'print "A"x1050'`
bash-2.03$ /usr/openwin/bin/Xsun :1
Warning: There is no XDISPLAY information for display 1.
Server is using XDISPLAY information for display 0.
Default Font Path: /usr/openwin/lib/X11/
Segmentation Fault (core dumped)
```

Sun Microsystems[3] está trabajando en los parches necesarios para solventar este agujero de seguridad, pero ahora mismo la única forma de "evitar" que saquen provecho del buffer overflow es quitar el bit SUID a Xsun (*chmod -s /usr/openwin/bin/Xsun*). De esta manera, aunque alguien se aproveche del buffer overflow, no obtendrá provilegios de root.

Lista de enlaces de este artículo:

1. http://www.eeye.com
2. http://www.eeye.com/html/Research/Advisories/solxsun.html
3. http://www.sun.com

E-mail del autor: daneel _ARROBA_ bulma.net
Podrás encontrar este artículo e información adicional en: http://bulma.net/body.phtml?nIdNoticia=606