



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

Actualiza urgentemente tu OpenSSH a la versión 3.3/3.4 (8527 lectures)

Per **Carlos Cortes Cortes**, [carcoco](http://bulma.net/~carcoco/) (<http://bulma.net/~carcoco/>)

Creado el 25/06/2002 20:21 modificado el 25/06/2002 20:21

Se ha descubierto una grave vulnerabilidad en **OpenSSH**, por lo que se recomienda una urgente actualización a la nueva **versión 3.3**. El problema ha levantado bastante revuelo y el propio **Theo de Raadt** (OpenBSD y OpenSSH) parece que se ha mosqueado un poco ...

Actualización: Ya esta disponible la nueva OpenSSH 3.4 que soluciona la vulnerabilidad **OpenSSH Remote Challenge Vulnerability**.

Según parece, no le han hecho mucho caso a [Theo](#)⁽¹⁾, he incluso algunos distribuidores **Linux** lo han ignorado, de todas formas, la nueva versión no soluciona el problema (que por cierto aún no ha sido explicado), sino que más bien lo minimiza en espera del parche definitivo.

De Raadt has been pushing to make privilege separation a de facto standard in distributions which include OpenSSH, but said in his announcement yesterday that he had met with consternation in the open source community.

"We've been trying to warn vendors about the need for privilege separation, but they really have not heeded our call for assistance. They have basically ignored us," he said in an email to the community.

La idea de **Theo** es ejecutar un parte del demonio **sshd** como un usuario no privilegiado, en lugar de ejecutarlo todo como **root**, de forma que reduzca la posibilidad y los riesgos en caso de un posible exploit, como el que se acaba de descubrir recientemente.

Tendremos que bajarnos la última versión del openssh, actualmente la [openssh-3.3p1.tar.gz](#)⁽²⁾, una vez compilada, tendremos que configurarla usando la opción (en el fichero `/etc/ssh/sshd_config`):

```
UsePrivilegeSeparation yes
```

OpenSSH: <http://www.openssh.com/>⁽³⁾

Más información sobre el tema:

- [openssh-unix-announce] Re: Upcoming OpenSSH vulnerability
<http://www.mindrot.org/pipermail/openssh-unix-announce/2002-June/000041.html>⁽⁴⁾
- Developers issue OpenSSH alert
[Developers issue OpenSSH alert](#)⁽⁵⁾
- Privilege Separated OpenSSH
<http://www.citi.umich.edu/u/provos/ssh/privsep.html>⁽⁶⁾
- Debian GNU/Linux Advisory: OpenSSH
http://linuxtoday.com/news_story.php3?itsn=2002-06-25-011-26-SC-DB⁽⁷⁾
- Slashback: OpenSSH, Bio, Timeliness
<http://slashdot.org/articles/02/06/24/1912215.shtml?tid=167>⁽⁸⁾



Actualización: Disponible la nueva versión 3.4 que soluciona la vulnerabilidad **OpenSSH Remote Challenge Vulnerability**.

Teneis más información sobre el tema en el [ISS advisory](#)⁽⁹⁾ y en el [OpenSSH advisory](#)⁽¹⁰⁾, del mismo modo que no esta de más hechar un vistazo por la noticia en Barrapunto ;-)

--

```
$ alias carcoco="echo Carlos Cortes"  
http://bulma.net/todos.phtml?id\_autor=132 (11)
```

Lista de enlaces de este artículo:

1. <http://www.theos.com/deraadt/>
2. <http://packetstorm.linuxsecurity.com/crypt/ssh/openssh/openssh-3.3p1.tar.gz>
3. <http://www.openssh.com/>
4. <http://www.mindrot.org/pipermail/openssh-unix-announce/2002-June/000041.html>
5. <http://www.vnunet.com/News/1132962>
6. <http://www.citi.umich.edu/u/provos/ssh/privsep.html>
7. http://linuxtoday.com/news_story.php3?tsn=2002-06-25-011-26-SC-DB
8. <http://slashdot.org/articles/02/06/24/1912215.shtml?tid=167>
9. <http://www.openssh.org/txt/iss.adv>
10. <http://www.openssh.org/txt/preauth.adv>
11. http://bulma.net/todos.phtml?id_autor=132

E-mail del autor: carcoco_ARROBA_gmail.com

Podrás encontrar este artículo e información adicional en: <http://bulma.net/body.phtml?nIdNoticia=1391>