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

Un gusano ataca máquinas linux (Apache/SSL) (16406 lectures)

Per **Carlos Cortes Cortes**, ***carcoco*** (http://bulma.net/~carcoco/)

Creado el 20/09/2002 10:46 modificado el 20/09/2002 10:46

> En los últimos días se ha propagado un **gusano** a través de máquinas **linux** (**NO actualizadas**), debido a un problema[1] en la implementación **SSL** del paquete **OpenSSL**, que afecta entre otros, al servidor web más utilizado en Internet; **Apache**, concretamente al modulo **mod_ssl**. Hay referencias al **gusano** con estos nombres: **Apache/mod_ssl worm, linux.slapper.worm, bugtraq.c worm, Modap worm, Linux.Slapper-A y Slapper.source ...**

Con este lio de nombres, no es de extrañar que exista cierta confusión, por eso, lo más sencillo para evitar equivocaciones es utilizar el CVE[2], que lo ha identificado como CAN-2002-0656[3], donde encontraremos todas las referencias al gusano.
"Buffer overflows in OpenSSL 0.9.6d and earlier, and 0.9.7-beta2 and earlier, allow remote attackers to execute arbitrary code via (1) a large client master key in SSL2 or (2) a large session ID in SSL3."

Según parece[4], tal y como comenta **Sandu Mihai**, simplemente teniendo la precaución de montar el directorio **/tmp** con **noexec** y **nosuid**, hubiera bloqueado este gusano y otros ataques similares ;-).
"Usually, a common tactical move is to securely design the system from the start. A /tmp placed on an independent partition, and mounted noexec, nosuid along with chattr +a on logs, and +i on important directories like /sbin, /bin and the like it is a fair policy."

Hay mucha información sobre el dichosos **gusano**, por lo que no voy a enrollarme sobre el tema, tan solo recomendaros que os actualiceis la versión del **Apache** (1.3.26 o 2.0.40 o superior) y **SSL** (0.9.6e o superior) lo antes posible, si no lo habeís hecho ya ;-)

Referencias:

- El virus Apache.Slapper. Worm para Linux infecta 6.000 servidores.
  http://www.lawebdelprogramador.com/noticias/mostrar.php?id=429[5]
- Apache_mod_ssl Worm Alert.
  http://securityresponse.symantec.com/avcenter/security/Content/2002.09.13.html[6]
- CAN-2002-0656 (under review).
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0656[3]
- OpenSSL SSLv2 Malformed Client Key Remote Buffer Overflow Vulnerability.
  http://online.securityfocus.com/bid/5363[7]
- CERT: Vulnerability Note VU#102795.
  OpenSSL servers contain a buffer overflow during the SSL2 handshake process
  http://www.kb.cert.org/vuls/id/102795[8]
- CERT Advisory CA-2002-23 Multiple Vulnerabilities In OpenSSL.
  http://www.cert.org/advisories/CA-2002-23.html[9]
- CERT Advisory CA-2002-27 Apache/mod_ssl Worm.
  http://www.cert.org/advisories/CA-2002-27.html[10]
- Linux.Slapper.Worm (Symantec).
  http://securityresponse.symantec.com/avcenter/venc/data/linux.slapper.worm.html[11]
- Linux.Slapper.Worm--What Red Hat customers can do about it.
  http://www.redhat.com/support/alerts/linux_slapper_worm.html[12]

- SecurityFocus has completed and released a full analysis (formato PDF).
  http://analyzer.securityfocus.com/alerts/020916-Analysis-Modap.pdf[13]
- That OpenSSL Worm (lwn.net).
  http://lwn.net/Articles/10119/[14]
- Remote detection of vulnerable OpenSSL versions.
  http://lwn.net/Articles/10205/[15]
  http://cert.uni-stuttgart.de/advisories/openssl-sslv2-master/openssl-sslv2-master.c[16]
- Global Slapper Worm Information Center.
  http://www.f-secure.com/slapper/[17]
- F-Secure Virus Descriptions (Slapper).
  Alias: Linux.Slapper-A, Linux.Slapper-Worm, Apache/ mod_ssl Worm, Slapper.source
  http://www.f-secure.com/v-descs/slapper.shtml[18]
- Slapped Silly (Securityfocus).
  http://online.securityfocus.com/columnists/109[19]
- Servidor Apache.
  http://httpd.apache.org/[20]
- OpenSSL.
  http://www.openssl.org/[21]

Gallir nos comenta esto sobre el **gusano** en un correo a la lista de **Bulma**:
"Pero si tenéis una versión menor de las openssl 0.9.6.e, actualizad ya, y mirad que vuestro ordenador no esté infectado con el puto gusano.

*Hay que mirar en /tmp por los ficheros **.cynik** y **.unlock***
*Si es así, actualizad vuestras libreráis **OpenSSL** (libssl0.9.6 en Debian) y reiniciad el apache, ssh y todo los demonios que la usen.*
***ALERTA**: aunque hayáis actualizado, si no re-arrancáis, el sistema sigue siendo vulnerable.*
De paso, haced:

```
tcpdump  udp  -x -n -s 64 port radius
```

Si véis mucho tráfico, ya sabéis :-("

--
carcoco
http://bulma.net/todos.phtml?id_autor=132[22]

Lista de enlaces de este artículo:

1. http://bulma.net/body.phtml?nIdNoticia=1429
2. http://bulma.net/body.phtml?nIdNoticia=1426
3. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0656
4. http://online.securityfocus.com/archive/1/291807
5. http://www.lawebdelprogramador.com/noticias/mostrar.php?id=429
6. http://securityresponse.symantec.com/avcenter/security/Content/2002.09.13.html
7. http://online.securityfocus.com/bid/5363
8. http://www.kb.cert.org/vuls/id/102795
9. http://www.cert.org/advisories/CA-2002-23.html
10. http://www.cert.org/advisories/CA-2002-27.html
11. http://securityresponse.symantec.com/avcenter/venc/data/linux.slapper.worm.html
12. http://www.redhat.com/support/alerts/linux_slapper_worm.html
13. http://analyzer.securityfocus.com/alerts/020916-Analysis-Modap.pdf
14. http://lwn.net/Articles/10119/
15. http://lwn.net/Articles/10205/
16. http://cert.uni-stuttgart.de/advisories/openssl-sslv2-master/openssl-sslv2-maste
17. http://www.f-secure.com/slapper/
18. http://www.f-secure.com/v-descs/slapper.shtml

19. http://online.securityfocus.com/columnists/109
20. http://httpd.apache.org/
21. http://www.openssl.org/
22. http://bulma.net/todos.phtml?id_autor=132

E-mail del autor: carcoco _ARROBA_ gmail.com