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

Problemas con OpenSSL, actualizate ya! (9542 lectures)

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

Creado el 02/08/2002 00:11 modificado el 02/08/2002 00:11

> Se han descubierto graves vulnerabilidades en las versiones 0.9.6d y 0.9.7-beta2 (y anteriores) de **OpenSSL**, por lo que se recomienda la **actualización** urgente. **OpenSSL** es una implementación libre y abierta de los protocolos **SSL v2/v3** (Secure Sockets Layer) y **TLS v1** (Transport Layer Security), ampliamente utilizados en **Internet**, sobretodo en todo el tema de **transacciones seguras** ...

En total han sido 4 problemas, que han sido referenciados en el CVE[1] como: CAN-2002-0656[2], CAN-2002-0655[3] y CAN-2002-0657[4], como podeís ver, esto del CVE[1], es realmente útil y eficaz ;-)

- **CAN-2002-0656**: 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.
- **CAN-2002-0655**: OpenSSL 0.9.6d and earlier, and 0.9.7-beta2 and earlier, does not properly handle ASCII representations of integers on 64 bit platforms, which could allow attackers to cause a denial of service and possibly execute arbitrary code.
- **CAN-2002-0657**: Buffer overflow in OpenSSL 0.9.7 before 0.9.7-beta3, with Kerberos enabled, allows attackers to execute arbitrary code via a long master key.

Podeís bajaros el **código fuente** de alguno de los mirror que encontrareís en http://www.openssl.org/source/[5], aunque yo os recomiendo que os paseís por la web de vuestra distribución y os bajeís directamente el paquete o paquetes que esten relacionados con el **OpenSSL**. Puesto que, por ejemplo, el propio **Apache** esta directamente relacionado, al ser habitual el tenerlo compilado con soporte para **OpenSSL**.

OpenSSL: http://www.openssl.org[6]

Mirrors para la descarga: http://www.openssl.org/source/[5]

--
$ alias **carcoco**="echo Carlos Cortes"
http://bulma.net/todos.phtml?id_autor=132 [7]

Lista de enlaces de este artículo:

1. http://bulma.net/ body.phtml?nIdNoticia=1426
2. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0656
3. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0655
4. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0657
5. http://www.openssl.org/source/
6. http://www.openssl.org
7. 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=1429