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

CVE: Common Vulnerabilities and Exposures (10111 lectures)

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

Creado el 30/07/2002 23:15 modificado el 30/07/2002 23:15

> **CVE** es un sigla que empieza a verse cada vez más junto a los últimas **vulnerabilidades/exploits** encontrados, independientemente del tipo de problema o del sistema operativo al que hagan referencia. Basicamente consiste en definir una forma común y estandar de llamar a las **vulnerabilidades/exploits** ...

La lista esta dividida en 2 partes: las vulnerabilidades ya aceptadas y que forman parte del **CVE** (Common Vulnerabilities and Exposures) y las que aún no han sido revisadas/aprobadas y se denominan **CANdidatas**. La revisión y control de la lista se lleva a cabo por el denominado **CVE Editorial Board**, que es un conjunto de expertos[1], entre los que se encuentran gente de la **NSA, Cisco, SANS Institute, Cerias, CanCERT, SecurityFocus, Red Hat, IBM** etc ...

¿Como se nombran cada entrada en esta lista?
El nombre de la vulnerabilidad es muy sencillo, **CVE** o **CAN**, el año y un número consecutivo dentre de ese año, por ejemplo: **CVE-2002-0083**, o **CAN-2002-0656** (que en el caso de ser aceptada, pasaría a denominarse **CVE-2002-0656**).

¿Qué compone cada entrada en el **CVE**?
Esta compuesta por el nombre, tal como he explicado antes, una descripción breve del problema y una lista de referencia a las fuentes oficiales del problema, por ejemplo:

```
Nombre:
CVE-2002-0083

Descripción:
Off-by-one error in the channel code of OpenSSH 2.0 through 3.0.2
allows local users or remote malicious servers to gain privileges.

Referencias:
VULNWATCH:20020307 [VulnWatch] [PINE-CERT-20020301] OpenSSH off-by-one
BUGTRAQ:20020307 OpenSSH Security Advisory (adv.channelalloc)
BUGTRAQ:20020307 [PINE-CERT-20020301] OpenSSH off-by-one
BUGTRAQ:20020308 [OpenPKG-SA-2002.002] OpenPKG Security Advisory (openssh)
BUGTRAQ:20020311 TSLSA-2002-0039 - openssh
BUGTRAQ:20020310 OpenSSH 2.9.9p2 packages for Immunix 6.2 with latest fix
BUGTRAQ:20020328 OpenSSH channel_lookup() off by one exploit
CONFIRM:http://www.openbsd.org/advisories/ssh_channelalloc.txt
ENGARDE:ESA-20020307-007
SUSE:SuSE-SA:2002:009
CONECTIVA:CLA-2002:467
DEBIAN:DSA-119
REDHAT:RHSA-2002:043
MANDRAKE:MDKSA-2002:019
NETBSD:NetBSD-SA2002-004
CALDERA:CSSA-2002-SCO.10
CALDERA:CSSA-2002-SCO.11
CALDERA:CSSA-2002-012.0
FREEBSD:FreeBSD-SA-02:13
HP:HPSBTL0203-029
XF:openssh-channel-error(8383)
BID:4241
```

Como dicen muy claramente no es una base de datos de vulnerabilidades, sino más bien una especie de **listado**/diccionario de vulnerabilidades con referencias a los **anuncios/avisos** oficiales desarrollados por una gran multitud de empresas o entidades relacionadas con la seguridad informática, tales como:
AIXAPAR, ALLAIRE, ASCEND, ATSTAKE, AUSCERT, BID, BINDVIEW, BUGTRAQ, CALDERA, CERT, CERT-VN, CHECKPOINT, CIAC, CISCO, COMPAQ, CONECTIVA, CONFIRM, DEBIAN, EEYE, EL8, ENGARDE, ERS, FarmerVenema, FreeBSD, HERT, HP, IBM, IMMUNIX, INFOWAR, ISS, KSRT, L0PHT, MANDRAKE, MISC, MS, MSKB, NAI, NETBSD, NETECT, NTBUGTRAQ, NetBSD, OPENBSD, REDHAT, RSI, SCO, SEKURE, SF-INCIDENTS, SGI, SNI, SUN, SUNBUG, SUSE, TURBO LINUX, URL, VULN-DEV, VULNWATCH, WIN2KSEC y XF
Aquí teneís esta impresionante lista, detallada con las direcciones donde obtener más información y avisos relativos a seguridad:
http://cve.mitre.org/cve/refs/refkey.html[2]

CVE is a list of information security vulnerabilities and exposures that aims to provide common names for publicly known problems. The goal of CVE is to make it easier to share data across separate vulnerability databases and security tools with this "common enumeration."

La última versión disponible es la **20020625**, es decir la del 25 de Junio del 2002, que contiene 2223[3] entradas *oficiales* y 2613[4] candidatas, una cifra bastante importante. Estoy seguro que esfuerzos como el que supone el **CVE** puedan ayudar a mejorar la seguridad de nuestro sistema informático, porque permite identificar de forma univoca cualquier **vulnerabilidad informática**.

Common Vulnerabilities and Exposures
http://cve.mitre.org/[5]
CVE Faq
http://cve.mitre.org/about/faq.html[6]

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

Lista de enlaces de este artículo:

1. http://cve.mitre.org/board/boardmembers.html
2. http://cve.mitre.org/cve/refs/refkey.html
3. http://cve.mitre.org/cve/
4. http://cve.mitre.org/cve/candidates/
5. http://cve.mitre.org/
6. http://cve.mitre.org/about/faq.html
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=1426