

INSEGURIDADES

SiteBar

SiteBar es una aplicación PHP que permite a los usuarios almacenar sus bookmarks o marcadores en un servidor web. Se han identificado distintos problemas en SiteBar que podrían permitir que se ejecutara código arbitrario o que se revelaran ficheros arbitrarios. El módulo de traducción no desinfecta adecuadamente el valor del parámetro *dir*. (CVE-2007-5491, CVE-2007-5694). El módulo de traducción tampoco desinfecta los valores de los parámetros *edit* y *value* que pasa a *eval ()* y *include ()*. (CVE-2007-5492, CVE-2007-5693)

El comando log-in no valida la URL a la que redirecciona a los usuarios después de registrarse. (CVE-2007-5695)

SiteBar también contiene algunas vulnerabilidades de scripting multisitio. (CVE-2007-5692) ■

Gentoo: GLSA 200711-05

OpenSSL

Un error "Off-by-one" en la implementación DTLS en OpenSSL 0.9.8 anterior a la 0.9.8f permite a los atacantes ejecutar código arbitrario mediante vectores inespecíficos. (CVE-2007-4995) ■

Fedora: Fedora-2007-725

Gentoo: GLSA 200710-30

Red Hat: RHSA-2007:0964

SUSE: SUSE-SR:2007:021

Ubuntu: USN-534-1

zope-cmfplone

Plone 2.5 hasta 2.5.4 y 3.0. hasta 3.0.2 permite a atacantes remotos ejecutar código Python arbitrario a través de datos de la red que contienen objetos pickled para los mensajes de estado o módulo de integridad de enlaces, con el que el módulo se descomprime y ejecuta. (CVE-2007-5741) ■

Debian: DSA-1405-1

Mono

Mono proporciona el software necesario para desarrollar y ejecutar clientes .NET y aplicaciones servidor en varias plataformas. La implementación BigInteger de Mono contiene una vulnerabilidad de desbordamiento de búfer que posible-

mente pudiera llevar a que se ejecutara código arbitrario.

Un atacante remoto podría explotar esta vulnerabilidad mediante el envío de datos especialmente manipulados a aplicaciones Mono usando la clase BigInteger, lo que podría conducir a la ejecución de código arbitrario con los privilegios de un usuario que ejecutara la aplicación (posiblemente root) o a una Denegación de Servicio. (CVE-2007-5197) ■

Debian: DSA-1397

Gentoo: GLSA 200711

SUSE: SUSE-SR:2007:023

phpMyAdmin

Se han descubierto algunas vulnerabilidades en phpMyAdmin, una aplicación que administrara MySQL en la red. phpMyAdmin permite que un atacante remoto inyecte script web arbitrariamente o HTML en el contexto de una sesión de registro de usuario (scripting multisitio). (CVE-2007-5589)

phpMyAdmin, cuando se accede a través de un navegador que no solicita URL codificada, permite que atacantes remotos inyecten script web arbitrariamente o HTML mediante la cadena de solicitud. (CVE-2007-5386) ■

Debian: DSA-1403

Plugins Nagios

Dos vulnerabilidades en los Plugins Nagios podrían permitir la ejecución remota de código arbitrario. Los Plugins Nagios son un juego oficial de plugins para Nagios, un programa de monitorización de red.

Un error de comprobación de límite en el plugin *check_snmp* cuando procesa respuestas *SNMP GET* podría llevar a un desbordamiento de búfer basado en pila (CVE-2007-5623). Un error de comprobación en la función *redir()* del plugin *check_http* cuando procesa información de encabezamiento HTTP *Location*: podría conducir a un desbordamiento de búfer (CVE-2007-5198) ■

Gentoo: GLSA 200711-11

Perl

Se ha descubierto un fallo en el motor de expresión regular de Perl. Una entrada a

una expresión regular especialmente manipulada puede hacer que Perl asigne memoria incorrectamente, teniendo como resultado la posible ejecución de código arbitrario con los permisos de un usuario ejecutando Perl. (CVE-2007-5116) ■

Debian: DSA-1400-1

Mandriva: MDKSA- 2007-207

Red Hat: RHSA-2007:0966-5,

RHSA-2007:1011-3

Kernel de Linux

Un subdesbordamiento de entero en la función *ieee80211_rx* en *net/ieee80211/ieee80211_rx.c* en el kernel de Linux 2.6.x previo a 2.6.23 permite a los atacantes remotos causar una denegación de servicio (se cuelga) a través de un valor de corrección *SKB* manipulado en un frame IEEE 802.11 cuando se configura el parámetro *IEEE80211_STYPE_QOS_DATA*. (CVE_2007-4997) ■

Debian: DSA-1381-2

SUSE: SUSE-SA:2007:059

PCRE

Múltiples desbordamientos de entero en la librería Perl-Compatible Regular Expressions (PCRE) anterior a 6.7 permite a atacantes dependientes del contexto ejecutar código arbitrario a través de una expresión regular que contiene un gran número de submodelos denominados (*name_count*), submodelos largos llamados (*max_name_size*), un submodelo repetido con un nombre largo, o un vector no específico implicando a las variables *max*, *min* y *duplength* en el largo cálculo en *pcre_compile*. (CVE-2006-7224) ■

Red Hat: RHSA-2007:1052-4

OpenLDAP

Se ha encontrado un fallo en la manera en la que el demonio *slapd* de OpenLDAP manipulaba los atributos LDAP de *objectClasses* malformados. Un atacante podría crear una petición LDAP que podría causar una denegación de servicio haciendo que se colgara *slapd* (CVE-2007-5707) ■

Mandriva: MDKSA- 2007-215

Red Hat: RHSA-2007:1037-3