

INSEGURIDADES

Adobe Flash Player

Las vulnerabilidades en Adobe Flash Player, una aplicación multimedia disponible en la mayoría de los navegadores web más comunes, podría ser explotada por atacantes para evitar restricciones de seguridad, revelar información sensible, ejecutar código de scripting arbitrario, o tomar el control completo de un sistema afectado.

Se encontraron algunos fallos de validación de entrada en la manera en la que Flash Player presenta determinado contenido, de modo que podría ejecutarse código arbitrario en la máquina de la víctima si ésta abre un fichero Adobe Flash malicioso. (CVE-2007-6242)

Flash Player usa permisos inseguros de memoria cuando se ejecuta en Linux, lo que podría permitir que los usuarios locales escalaran privilegios. (CVE-2007-6246)

Un desbordamiento de búfer basado en pila en la librería Perl-Compatible Regular Expression (PCRE) anterior a la versión v7.3 permite a los atacantes dependientes del contexto ejecutar código arbitrario a través de una secuencia singleton Unicode en una clase de carácter en un modelo regex que se haya optimizado incorrectamente. Esto puede causar un error en Flash Player que derivaría en una vulnerabilidad. (CVE-2007-4768)

El plugin Adobe Macromedia Flash 9 permite a los atacantes remotos hacer que una máquina víctima establezca sesiones TCP con servidores arbitrarios a través de una película Flash (SWF). Un atacante remoto podría usar luego Flash Player para llevar a cabo un ataque DNS vinculante. (CVE-2007-5275)

ActionScript 3 (AS3) en Adobe Flash Player permite a atacantes remotos evitar el Security Sandbox Model (Modelo Cajón de arena de Seguridad), obtener información sensible, y portar hosts falsos arbitrarios mediante una película Flash (SWF) que especifique una conexión por realizar. Pueden usarse discrepancias de coordinación del error *SecurityErrorEvent* para determinar si un puerto está abierto. (CVE-2007-4324)

Atacantes remotos podrían inyectar script web mediante un fichero SWF que

usa el protocolo *asfunction* de la función *navigateToURL* cuando se usa con Flash Player ActiveX Control en Internet Explorer como resultado de múltiples vulnerabilidades de scripting multisitio. (CVE-2007-6244)

Se encontró un fallo en la manera en la que Flash Player modificaba encabezamientos de peticiones http. Atacantes remotos podrían modificar encabezamientos http y usar Flash Player para llevar a cabo un ataque de respuesta dividida http. (CVE-2007-6245) ■

Red Hat: RHSA-2007:1126
SUSE: SUSE-SA:2007:069

Libsndfile

Una vulnerabilidad en Libsndfile, una librería C para lectura y escritura de ficheros audio, está causada por un error de desbordamiento de búfer en la función *flac_buffer_copy()* [*flac.c*] cuando procesa un fichero FLAC con datos PCM especialmente manipulados. Esto podría ser explotado por atacantes remotos para comprometer un sistema afectado engañando a un usuario para que abriera un fichero malicioso con el uso de una aplicación vinculada contra una librería vulnerable. (CVE-2007-4974) ■

Debian: DSA-1442-2
Fedora: FEDORA-2007-2236
Gentoo: GLSA 200710-04
Mandrake: MDKSA-2007:191
Ubuntu: USN-525-1

Plone

Una vulnerabilidad en Plone podría ser explotada por atacantes remotos para comprometer un sistema vulnerable y ejecutar comandos con los privilegios de procesos Zope/Plone. La vulnerabilidad está causada por errores de validación de entrada en los módulos que interpretan datos de la red inseguros. (CVE-2007-5741) ■

Debian: DSA-1405-3, DSA-1405-1, DSA-1405-2

Samba

Una vulnerabilidad en Samba podría ser explotada por atacantes remotos para causar una denegación de servicio o

para ejecutar código arbitrario. El problema se encuentra en la manera en la que Samba autentifica usuarios remotos. Un error de desbordamiento de búfer en la función *send_mailslot()* mientras procesa un paquete logon de dominio SAMLOGON especialmente manipulado, conteniendo una cadena de nombre de usuario situada en un offset impar seguido por una cadena demasiado larga *getdc*, podría permitir que atacantes remotos comprometieran un sistema vulnerable o que éste se colgara. Esto ocurre cuando se encuentra habilitada la opción *domain logons*. (CVE-2007-6015) ■

Debian: DSA-1427-1
Fedora: FEDORA-2007-4269, FEDORA-2007-4275
Gentoo: GLSA 200712-10
Mandrake: MDKSA-2007:244
Red Hat: RHSA-2007:1114, RHSA-2007:1117
Slackware: SSA-2007-344-01
SUSE: SUSE:2007:068
Ubuntu: USN-556-1

ClamAV

Clam AntiVirus (ClamAV) es vulnerable a un desbordamiento de búfer basado en pila, el cual podría permitir que un atacante remoto ejecutara código arbitrario con privilegios escalados o causara una denegación de servicio. El desbordamiento está causado por un error en la función *cle_scanpe* cuando analiza ficheros PE empaquetados con el empaquetador MEW. (CVE-2007-6335)

Otra vulnerabilidad está causada por un error de desbordamiento de búfer off-by-one en el código de descompresión MS-ZIP, que podría ser explotado para ejecutar código arbitrario o para que se colgara una aplicación vulnerable. (CVE-2007-6336)

Una vulnerabilidad en el algoritmo de descompresión bzip2 en *nsis/bzlib_private.h* en ClamAV anteriores a 0.92 tiene efectos y vectores de ataque remoto desconocidos. (CVE-2007-6337) ■

Debian: DSA-1435-1
Gentoo: GLSA 200712-20
Ubuntu: USN-557-1