

# INSEGURIDADES

## ■ GnuPG

GnuPG es una utilidad para la encriptación de datos y la creación de firmas digitales.

Tavis Ormandy descubrió un fallo en la manera en la que GnuPG verifica los datos firmados criptográficamente con firmas separadas. Un atacante que conozca este fallo puede crear un mensaje firmado criptográficamente que podría parecer venir de un tercero.

Cuando una víctima procesa un mensaje GnuPG con una firma separada

malformada, GnuPG la ignora, procesa y produce los datos firmados, y sale con estado 0, tal y como si la firma hubiera sido válida.

En este caso, el estado de salida de GnuPG no debería indicar que ha tenido lugar una verificación de firmas. Este problema sería peligroso en el caso de que los resultados del proceso de GnuPG se obtuviesen a través de un script automatizado.

El Proyecto de Vulnerabilidades y Exposiciones Comunes (Common

Vulnerabilities and Exposures o CVE, <http://cve.mitre.org>) ha asignado a este problema el nombre CVE-2006-0455.

Tavis Ormandy también descubrió un fallo en la manera en la que GnuPG verifica los datos firmados criptográficamente con firmas inline. Es posible para un atacante introducir datos sin firmar en un mensaje firmado, de modo que cuando la víctima procese el mensaje para recuperar los datos, los que están sin firmar aparecen junto a los datos firmados. De esta manera los datos no firmados tienen la apariencia de haber sido firmados.

El Proyecto de Vulnerabilidades y Exposiciones Comunes (Common Vulnerabilities and Exposures o CVE, <http://cve.mitre.org>) ha asignado a este problema el nombre CVE-2006-0049. ■

*Referencia Debian: DSA-993-1,2*  
*Referencia Gentoo: GLSA-200603-08*  
*Referencia Mandriva: MDKSA-2006:055*  
*Referencia Red Hat: RHSA-2006:0266-8*  
*Referencia Slackware: SSA:2006-072-02*  
*Referencia Suse: SUSE-SA:2006:014*

## ■ Sendmail

Sendmail es un Agente de Transporte de Correo (MTA) usado para el envío de correo entre máquinas.

Se descubrió un fallo en la manipulación de señales asíncronas en Sendmail. Un atacante remoto podría explotar una condición de carrera para ejecutar código arbitrario como superusuario. El Proyecto de Vulnerabilidades y Exposiciones Comunes (Common Vulnerabilities and Exposures o CVE, <http://cve.mitre.org>) ha asignado a este problema el nombre CVE-2006-0058.

Mediante esta vulnerabilidad solamente podría ser explotado los servidores configurados para que Sendmail escuchara hosts remotos. ■

*Referencia Debian: DSA-1015-1*  
*Referencia Gentoo: GLSA-200603-21*  
*Referencia Mandriva: MDKSA-2006:058*  
*Referencia Red Hat: RHSA-2006:0264-8*  
*Referencia Slackware: SSA:2006-081-01*  
*Referencia Suse: SUSE-SA:2006:017*

## POLITICAS DE SEGURIDAD DE LAS DISTRIBUCIONES MAYORITARIAS

Distribuidor	Fuente Seguridad	Comentario
Debian	Info: <a href="http://www.debian.org/security/">http://www.debian.org/security/</a> Lista: <a href="http://www.debian.org/debian-security-announce/">http://www.debian.org/debian-security-announce/</a> Referencia: DSA-... 1)	Los avisos de seguridad actuales se incluyen en la página de inicio. Los avisos se proveen como páginas HTML con enlaces a los parches. Los avisos también incluyen una referencia a la lista de correo.
Gentoo	Info: <a href="http://www.gentoo.org/security/en/index.xml">http://www.gentoo.org/security/en/index.xml</a> Foro: <a href="http://forums.gentoo.org/">http://forums.gentoo.org/</a> Lista: <a href="http://www.gentoo.org/main/en/lists.xml">http://www.gentoo.org/main/en/lists.xml</a> Referencia: GLSA-... 1)	Los avisos de seguridad actuales para la lista Gentoo en el sitio web de seguridad de Gentoo enlazan desde la página principal. Los avisos se presentan en HTML con códigos para fusionar las versiones corregidas.
Mandrake	Info: <a href="http://www.mandrakesecure.net">http://www.mandrakesecure.net</a> Lista: <a href="http://www.mandrakesecure.net/en/mlist.php">http://www.mandrakesecure.net/en/mlist.php</a> Referencia: MDKSA-... 1)	Mandrakesoft posee su propios sitio web que versa sobre temas relacionados con la seguridad. Entre otras cosas, incluye avisos seguridad y referencias a las listas de correo. Los avisos son páginas HTML, pero no contienen enlaces a los parches.
Red Hat	Info: <a href="http://www.redhat.com/errata/">http://www.redhat.com/errata/</a> Lista: <a href="http://www.redhat.com/mailman/listinfo/">http://www.redhat.com/mailman/listinfo/</a> Referencia: RHSA-... 1)	Red Hat archiva los fallos de seguridad bajo lo que denominan <i>erratas</i> . A continuación los problemas para cada versión de Red Hat se agrupan. Los avisos de seguridad se proveen como una página HTML con enlaces a los parches.
Slackware	Info: <a href="http://www.slackware.com/security">http://www.slackware.com/security</a> Lista: <a href="http://www.slackware.com/lists/slackware-security">http://www.slackware.com/lists/slackware-security</a> Referencia: [slackware-security]... 1)	La página de inicio contiene enlaces al archivo de seguridad de la lista de correo. No existe información adicional sobre seguridad en Slackware.
Suse	Info: <a href="http://www.suse.de/en/private/support/security/index.html">http://www.suse.de/en/private/support/security/index.html</a> Parches: <a href="http://www.suse.de/en/private/download/updates">http://www.suse.de/en/private/download/updates</a> Lista: suse-security-announce Referencia: SUSE-SA-... 1)	Ya no existe un enlace a la página de seguridad tras un remodelado en el sitio web de SuSE. Existe información en la lista de correos y los avisos. Los parches de seguridad para versiones individuales de SuSE Linux se muestran de color rojo en el sitio de actualizaciones generales. Contiene una corta descripción de la vulnerabilidad que soluciona el parche.

1) Todos los distribuidores muestran correos de seguridad en el campo *Subject*.

■ Zoo

Zoo es una utilidad de archivado de ficheros escrita por Rahul Dhesi para el mantenimiento de colecciones de ficheros. Zoo es vulnerable a un nuevo desbordamiento de búfer debido al uso inseguro de la función `strcpy()` cuando intenta crear un archivo desde determinados directorios o nombres de ficheros.

Un atacante podría explotar este problema persuadiendo a un usuario para que cree un archivo zoo de directorios y ficheros especialmente manipulados, permitiendo así la ejecución de código arbitrario con los derechos del usuario que ejecuta zoo.

Referencia Debian: DSA-991-1  
Referencia Gentoo: GLSA-200603-12  
Referencia Suse: SUSE-SR:2006:006

■ X.org-x11

Un fallo de programación en el Servidor X.Org X permite a atacantes locales conseguir privilegios de superusuario cuando el servidor es root setuid, tal y como ocurre en la configuración por

defecto de SUSE Linux 10.0. Este fallo fue descubierto por el proyecto Coverity.

Solamente se encuentra afectado SUSE 10.0; los productos anteriores a él no incluyen el fragmento de código problemático.

El problema está siendo seguido por Mitre CVE ID CVE-2006-0745.

Referencia Mandriva: MDKSA-2006:056  
Referencia Suse: SUSE-SA:2006:016

■ OpenOffice

OpenOffice.org es una suite de productividad ofimática. Contiene herramientas de productividad tales como un procesador de texto, hoja de cálculo, etc. Otras herramientas incluyen presentaciones, edición de fórmulas, exploración de datos y conversión de ficheros. lib-curl, que se encuentra incluido en OpenOffice.org, es una librería libre y de fácil uso por el lado del cliente para la transferencia de ficheros con sintaxis URL. Dicha librería incluye numerosos protocolos.

OpenOffice.org posee código libcurl. Dicho código es vulnerable a un

desbordamiento de pila cuando intenta analizar una URL que excede el límite de 256 Byte (GLSA 200512-09).

Un atacante conocedor de este problema con libcurl podría tentar a un usuario para que invocara a una URL especialmente manipulada con OpenOffice.org, produciendo de manera potencial la ejecución de código arbitrario con los derechos de un usuario que está corriendo la aplicación.

Referencia Gentoo: GLSA-200603-25

■ Flash Player

Ha sido identificada una vulnerabilidad de seguridad crítica en Adobe Macromedia Flash Player que permite a un atacante que explote dicha vulnerabilidad con éxito tomar el control de la aplicación corriendo flash player.

Para que un atacante explote dichas vulnerabilidades un usuario debe cargar un SWF malicioso en el Flash Player creado por el atacante.

Este problema está siendo seguido por Mitre CVE ID CVE-2006-0024.

# Descubre lo que te espera en la Red

Zona de descarga

Servicio al lector

Artículos descargables

Calendario de eventos

