Informe original del

SELESTA SEGURIDAD http://www.selseg.com

SANS Institute
A Cooperative Education & Research Organization

Cómo eliminar las diez vulnerabilidades de seguridad en Internet más críticas

El consenso de los expertos

Versión 1.27 - 12 de septiembre de 2000

¡Detener los accesos no autorizados!

La mayoría de los ataques con éxito a ordenadores mediante Internet se pueden agrupar como la utilización de un reducido número de vulnerabilidades. La mayor parte de los ordenadores comprometidos durante el incidente conocido como "Solar Sunrise Pentagon" fueron atacados mediante una vulnerabilidad concreta. Una vulnerabilidad similar a esa fue la que se utilizó para controlar la mayor parte de los ordenadores que posteriormente se utilizaron masivamente en los ataques distribuidos de negación de servicio. De la misma forma, los recientes accesos ilegales a servidores web basados en Windows NT están asociados a la utilización de una vulnerabilidad sobradamente conocida. Otra vulnerabilidad, todavía, suficientemente estudiada para ser la causa de permitir el control ilegal de más de 30.000 sistemas Linux.

Actualizaciones

v. 1.27 -12/08/00

Actualizacion del apéndice B.

v. 1.26 -21/08/00

Actualización de la URL de soporte de RedHat Linux.

v. 1.25 -12/07/00

Nuevo apéndice - Información de actualizaciones de distribuidores de Unix

v. 1.24 -11/07/00

Nueva sección con las personas que han colaborado en mejorar este documento.

v. 1.23 -11/07/00

Actualización de la relación de códigos CVE de la sección 2

v. 1.22 -19/06/00

Actualización de las firmas

Downloads

Documento en formato PDF (Adobe Acrobat)

Con sólo algunas vulnerabilidades, en definitiva, se realizan la mayor parte de los ataques con éxito debido, en gran parte a que los atacantes son oportunistas – utilizan la vía más fácil y conveniente. Utilizan las brechas mejor conocidas mediante el uso de diversas herramientas de ataques muy efectivas y ampliamente difundidas. Se aprovechan de aquellas organizaciones que no aplican los parches para resolver los problemas, realizando habitualmente ataques de forma indiscriminada, rastreando en Internet por la

existencia de sistemas vulnerables.

La mayor parte de los administradores de sistemas afirman que no han solucionado estas brechas de seguridad por la simple razón que desconocen cuales de los 500 problemas potenciales son los más peligrosos y carecen del tiempo necesario para poder corregirlos todos.

La comunidad de profesionales de la seguridad informática desea resolver este problema identificando las áreas de seguridad en Internet más críticas – el grupo de vulnerabilidades que los administradores de sistemas deben eliminar de forma inmediata. Esta lista consensuada, a la que denominaremos Top Ten, es un ejemplo sin precedentes de cooperación activa entre la industria, los organismos públicos y las instituciones educativas. Los participantes provienen de las agencias federales con mayor conciencia en temas de seguridad, de los principales distribuidores de productos de seguridad, de consultoras especializadas; de diversas universidades con programas especializados en seguridad y del CERT/CC y el SANS Institute. Al final del articulo incluimos la relación completa de participantes.

Esta es la lista de los 10 problemas de seguridad en Internet más frecuentemente utilizados, con la relación de acciones que deben tomarse para proteger los sistemas de las mismas.

Tres notas para el lector:

> **Nota 1**. Este es un documento en constante evolución. Incluye las instrucciones iniciales, paso a paso y direcciones para solucionar los defectos. Iremos actualizando las instrucciones a medida que vayamos identificando cuales son los pasos más convenientes; se agradecerán los comentarios del lector al respecto. Este documento es un consenso de la comunidad –su experiencia en la eliminación de las vulnerabilidades puede ayudar a los que vengan detrás. Para enviar sus sugerencias, envíe un mensaje a <barcelona@selseg.com> utilizando " **Comentarios al Top Ten**" como tema del mismo. Para obtener la versión más actualizada de estas instrucciones, envíe un mensaje a <barcelona@selseg.com> con el tema " **Documento Top Ten**".
>
> **Nota 2**. Encontrará referencia a registros CVE – los números de referencia de las Vulnerabilidades y Exposiciones más Habituales, que se corresponden con una vulnerabilidad. Los números CAN corresponden a propuestas de CVE que no han sido totalmente verificadas. Para información adicional sobre el proyecto CVE, visite http://cve.mitre.org.
>
> **Nota 3**. Al final de la lista, encontrará una sección extra con una relación de los puertos utilizados por los servicios habitualmente sondeados y atacados. Bloqueando el tráfico a dichos puertos en su cortafuegos u otro dispositivo de protección perimetral, obtendrá un nivel extra de defensa que le ayuda a protegerse de los errores de configuración.

Contenido

1. **Debilidades de BIND**: `nxt`, `qinv` e `in.named` permiten comprometer la cuenta de root inmediatamente.

2. **Programas CGI** y extensiones de aplicación (por ejemplo, ColdFusion) instalados en servidores web.

3. Debilidades en llamadas de procedimiento remoto (RPC) en rpc.ttdbserverd (ToolTalk), rpc.cmsd (Calendar Manager) y rpc.statd que permiten la obtención inmediata de privilegio de root.

4. Agujero de seguridad RDS en Microsoft Internet Information Server (IIS).

5. Debilidad por desbordamiento de buffer en sendmail; ataques mediante áreas de interconexión de memoria y MIMEbo; todas ellas permiten comprometer la cuenta de root inmediatamente.

6. sadmind y mountd.

7. Compartición de archivos global y compartición de información inapropiada mediante NetBIOS y los puertos 135 -> 139 en Windows NT (445 en Windows 2000), exports de NFS en Unix (puerto 2049), compartición vía web en Macintosh y Appleshare/IP en puertos 80, 427 y 548.

8. Cuentas de usuario, especialmente la de root o administrador, sin contraseña o con contraseña poco segura.

9. Vulnerabilidades de desbordamiento de buffer o configuración incorrecta en IMAP y POP3.

10. Nombres de comunidad SNMP por omisión ('public' y 'private').

Información adicional

- Un punto prioritario para los usuarios y/o administradores de Windows: varios agujeros de script en Internet Explorer y Office 2000.

- Protección perimetral para una línea adicional de defensa.

- Información de soporte de los diversos fabricantes de Unix

- Firmantes.

Debilidades de BIND: nxt, qinv e in.named permiten comprometer la cuenta de root inmediatamente

El paquete Berkeley Internet Name Domain (BIND), es la implementación más utilizada de servicio de nombres de dominio (DNS) -- el importante sistema que nos permite localizar los sistemas en Internet por su nombre (por ejemplo, www.sans.org) sin necesidad de utilizar direcciones IP -- lo que lo convierte en uno de los blancos favoritos para un ataque. Es triste ver que, de acuerdo con una encuesta realizada a mediados de 1999, cerca del 50% de todos los servidores de DNS conectados a Internet utilizaban una versión de BIND vulnerable. En un ataque típico a BIND, los intrusos borran los archivos log del sistema e instalan herramientas que les permiten obtener privilegios de administrador. A continuación, compilan e instalan diversas utilidades de IRC y escaneo de redes, que las utilizarán para encontrar (dentro del rango de varias clases B de direcciones IP) otros sistemas que también utilicen versiones vulnerables de BIND. En cuestión de minutos, habrán utilizado el sistema comprometido para atacar cientos de sistemas remotos, obteniendo el control de los mismos. Esto ilustra el caos que puede resultar de una simple vulnerabilidad en un software para la gestión de servicios universales en Internet, como puede ser el DNS.

Sistemas afectados
Diversos sistemas UNIX y Linux.

A fecha 22 de mayo de 2000, todas las versiones de BIND anteriores a la v.8.2.2 actualización 5 son vulnerables.

Registro CVE:
nxt CVE-1999-0833
qinv CVE-1999-0009

Otros registros CVE relacionados: CVE-1999-0835, CVE-1999-0848, CVE-1999-0849, CVE-1999-0851

Consejos para la resolución del problema:

- Desactivar el daemon BIND (named) en todos aquellos sistemas que no actúan como servidores de DNS. Algunos expertos incluso recomiendan la desinstalación del software de DNS.

- En máquinas que actúan como servidores de DNS, actualizar a la última versión (a 22 de mayo de 2000, la versión más reciente es la v.8.2.2 actualización 5).

  Puede seguir los consejos indicados en los siguientes avisos:

  Para la vulnerabilidad NXT: http://www.cert.org/advisories/CA-99-14-bind.html

  Para las vulnerabilidades QINV (pregunta inversa) y NAMED:
  http://www.cert.org/advisories/CA-98.05.bind_problems.html
  http://www.cert.org/summaries/CS-98.04.html

- Ejecute BIND como un usuario sin privilegios como medida de protección ante futuros ataques. (No obstante, sólo los procesos que se ejecutan como root pueden ser configurados para utilizar los puertos inferiores al 1024 –un requisito del DNS. Por tanto, deberá configurar BIND para que cambie de usuario una vez se haya asociado al puerto).

- Ejecute BIND en una estructura de directorios chroot() como medida de protección ante futuros ataques.

Programas CGI y extensiones de aplicación (por ejemplo, ColdFusion) instalados en servidores web.

Casi todos los servidores web dan soporte a programas CGI (Common Gateway Interface) para ofrecer páginas interactivas, tales como la obtención y verificación de datos. Muchos servidores incluyen diversos programas CGI de ejemplo que se instalan por omisión. Desafortunadamente, algunos programadores de CGIs no han considerado la posibilidad que sus programas pueden ser utilizados de forma incorrecta o ser engañados para ejecutar mandatos con fines maliciosos. Los CGIs vulnerables son un blanco particularmente atractivo para los intrusos ya que son relativamente fáciles de localizar y funcionan con los mismos privilegios y poder que el software del servidor web.

Se sabe que los intrusos se han aprovechado de CGIs vulnerables para modificar páginas web, robar información de tarjetas de crédito e instalar puertas traseras para posteriores intrusiones, incluso en el momento en que los CGIs ya han sido protegidos. Cuando la foto de Janet Reno fue sustituida por la de Adolph Hitler, un informe interno concluyó que la causa más probable para el ataque fue la utilización de un agujero de seguridad en un programa CGI.

ColdFusion de Allaire es un paquete de aplicaciones para servidores web que instala algunos programas de ejemplo con vulnerabilidades. Como norma general, los programas de ejemplo deben ser siempre eliminados de los sistemas de producción.

Sistemas afectados
Todos los servidores web

Registros CVE:

- **Programas CGI de ejemplo (todos los CGIs)**
  Remedio:
  Eliminar los programas CGI de ejemplo en los servidores de producción.

- **CAN-1999-0736**
  (Internet Information Server 4.0, Microsoft Site Server 3.0 --que se incluye en el Microsoft Site Server 3.0 Commerce Edition--, Microsoft Commercial Internet Server 2.0 y Microsoft BackOffice Server 4.0 y 4.5)
  consultar http://www.microsoft.com/technet/security/bulletin/ms99-013.asp

  Remedio:
  Aplicar el parche disponible en ftp://ftp.microsoft.com/bussys/iis/iis-public/fixes/usa/Viewcode-fix/

- **CVE-1999-0067**
  Programa de agenda escrito en phf incluido en versiones antiguas de los servidores NCSA y Apache.

- **CVE-1999-0068**
  Script de ejemplo 'mylog.html' incluido en PHP/FI.

- **CVE-1999-0270**
  IRIX 6.2, 6.3 y 6.4

- **CVE-1999-0346**
  Programas de ejemplo incluidos en el paquete PHP/FI.

- **CVE-2000-0207**
  IRIX 6.5

Vulnerabilidades de CGIs más importantes sin incluir los programas de ejemplo:

- **CAN-1999-0467**
  CGI de Libro de visitas de WebCom.

- **CAN-1999-0509 (aplicable a todos los servidores)**
  Consultar http://www.cert.org/advisoires/CA-96.11.interpreters_in_cgi_bin_dir.html

  Remedio:
  La solución a este problema es asegurarse que no se encuentre ninguna copia de los programas intérpretes de lenguajes propósito general, como por ejemplo PERL, TCL, shells de Unix (sh, csh, ksh, etc).

- **CVE-1999-0021**
  wwwcount versión 2.3

- **CVE-1999-0039**
  Subsistema Outbox de IRIX

- **CVE-1999-0058**
  Paquete PHP/FI.

- **CVE-1999-0147**
  Glimpse HTTP 2.0 y WebGlimpse.

- **CVE-1999-0148**
  Subsistema Outbox de IRIX.

- **CVE-1999-0149**
  Subsistema Outbox de IRIX.

- **CVE-1999-0174 (aplicable a todos los servidores)**
  Consultar http://xforce.iss.net/static/291.php y http://www.netscape.org/cgi-bin/wa?A2=ind9702B&L=bugtraq&P=R64

  Remedio:
  Eliminar el script 'view-source' del directorio cgi-bin del servidor web.

- **CVE-1999-0177**
  Website 2.0 de O'Reilly.

- **CVE-1999-0178**
  Website 2.0 de O'Reilly.

- **CVE-1999-0237**
  Libro de visitas de Webcom para servidores web en entorno Win32.

- **CVE-1999-0262**
  Fax Survey para sistemas Linux.

- **CVE-1999-0279**
  Excite for Web Servers.

- **CVE-1999-0771**
  Agente de gestión y utilidad de análisis de Compaq.

- **CVE-1999-0951**
  CGI OmniHTTPd

- **CVE-2000-0012**
  CGI del Microsoft SQL Server.

- **CVE-2000-0039**
  Sistema de búsqueda Altavista.

- **CVE-2000-0208**
  htsearch para ht://dig.

Vulnerabilidades en los programas de ejemplo de ColdFusion

- **CAN-1999-0455**

- **CAN-1999-0922**

- **CAN-1999-0923**

Otras vulnerabilidades de ColdFusion

- **CAN-1999-0760**

- **CVE-2000-0057**

Consejos para la resolución del problema:

- No ejecutar el servidor web como root

- Eliminar los intérpretes de scripts para CGIs de los directorios bin:
  http://www.cert.org/advisories/CA-96.11.interpreters_in_cgi_bin_dir.html

- Eliminar los scripts CGI no seguros:
  http://www.cert.org/advisories/CA-97.07.nph-test-cgi_script.html
  http://www.cert.org/advisories/CA-96.06.cgi_example_code.html
  http://www.cert.org/advisories/CA-97.12.webdist.html

- Escribir programas CGI seguros:
  http://www-4.ibm.com/software/developer/library/secure-cgi/
  http://www.cert.org/tech_tips/cgi_metacharacters.html
  http://www.cert.org/advisories/CA-97.24.Count_cgi.html

- No configurar el soporte de CGIs en aquellos servidores web que no lo necesiten.

- Ejecutar el servidor web en un entorno de directorios chroot para proteger la máquina de posibles ataques todavía no descubiertos.

Debilidades en llamadas de procedimiento remoto (RPC) en `rpc.ttdbserverd` (ToolTalk), `rpc.cmsd` (Calendar Manager) y `rpc.statd` que permiten la obtención inmediata de privilegio de root

Las llamadas de procedimiento remoto (RPC) permiten a los programas de un ordenador la ejecución de programas en un segundo ordenador. Se utilizan habitualmente para acceder a servicios de red tales como la compartición de archivos en NFS. Diversas vulnerabilidades originadas por brechas de RPC son explotadas de forma activa. Existe una evidencia convincente que la mayor parte de los ataques distribuidos de denegación de servicio efectuados durante 1999 y principios del 2000 fueron ejecutados por sistemas a los que se había comprometido debido a sus vulnerabilidades en programas RPC. El ataque -exitoso- general contra los sistemas del ejército de los EE.UU. ocurrido en el incidente 'Solar Sunrise' utilizó igualmente un error en un programa RPC presente en cientos de sistemas del departamento de defensa americano.

Sistemas afectados
Diversos sistemas UNIX y Linux.

Registro CVE:
rpc.ttdbserverd - CVE-1999-0687, CVE-1999-0003, CVE-1999-0693
(-0687 es más reciente que el -0003, pero ambos permiten a los atacantes remotos obtener privilegios de root y es bastante probable que el -0003 todavía es bastante frecuente; -0693 sólo puede utilizarse a nivel local, pero permite obtener privilegio de root)

rpc.cmsd – CVE-1999-0696

rpc.statd - CVE-1999-0018, CVE-1999-0019.

Consejos para la resolución del problema:

- Siempre que sea posible, desactivar y/o eliminar estos servicios en las máquinas que son directamente accesibles desde Internet.

- Cuando sea necesario utilizarlos, instalar los parches más recientes:

  Parches para sistemas Solaris:
  http://sunsolve.sun.com

  Para AIX de IBM:
  http://techsupport.services.ibm.com/support/rs6000.support/downloads
  http://techsupport.services.ibm.com/rs6k/fixes.html

  Para sistemas SGI:
  http://support.sgi.com/

  Para Compaq (Digital Unix):

http://www.compaq.com/support

Buscar en las bases de datos de parches de cada fabricante los parches para tooltalk e instalarlos de forma inmediata.

Un documento que resume los consejos específicos para cada una de las tres vulnerabilidades principales de RPC se encuentra en:
http://www.cert.org/incident_notes/IN-99-04.html

Para statdd:
http://www.cert.org/advisories/CA-99-05-statd-automountd.html

Para ToolTalk:
http://www.cert.org/advisories/CA-98.11.tooltalk.html

Para Calendar Manager:
http://www.cert.org/advisories/CA-99-08-cmsd.html

Agujero de seguridad RDS en Microsoft Internet Information Server (IIS)

Microsoft Internet Information Server (IIS) es el servidor web utilizado por la mayoría de servidores web instalados en la plataforma Windows NT y Windows 2000. Algunos errores en la programación de los servicios de datos remotos (Remote Data Services, RDS) son utilizados por usuarios con malas intenciones para ejecutar mandatos remotos con privilegio de administrador. Algunos de los participantes en la redacción de la lista "Top Ten" consideran que otras brechas del IIS, tales como los archivos .HTR, son por lo menos tan utilizadas como esta brecha del RDS. La prudencia recomienda a las organizaciones usuarias del IIS, aprovechar la instalación/actualización necesaria para solucionar el problema con RDS para la instalación de todos los parches y actualizaciones necesarios para solucionar todas las brechas de seguridad conocidas del IIS.

Sistemas afectados
Sistemas con Microsoft Windows NT que utilicen el Internet Information Server

Registro CVE:
CVE-1999-1011

Consejos para la resolución del problema:

- Una completa guia sobre esta debilidad y sobre como solucionarla, se encuentra disponible en

- Utilizar la información publicada por Microsoft para deshabilitar el servicio o solucionar la vulnerabilidad RDS y otros problemas de seguridad del IIS.
  http://support.microsoft.com/support/kb/articles/q184/3/75.asp
  http://www.microsoft.com/technet/security/bulletin/ms98-004.asp
  http://www.microsoft.com/technet/security/bulletin/ms99-025.asp

Debilidad por el desbordamiento de buffer en sendmail ataques mediante áreas de interconexión de memoria y MIMEbo; todas ellas permiten comprometer la cuenta root inmediatamente.

Sendmail es el programa más utilizado en sistemas UNIX y Linux para enviar, recibir y redireccionar el correo electrónico. La amplia utilización de Sendmail en Internet lo convierte en uno de los principales objetivos de los atacantes. A lo largo de los años, se han detectado diversos defectos. La primera recomendación emitida por el CERT/CC en 1988 hacía referencia a una debilidad explotable de sendmail. En uno de los ataques más habituales, el atacante envía un mensaje convenientemente formateado al sistema que ejecuta Sendmail; éste lo interpreta como un conjunto de instrucciones mediante las cuales la máquina víctima del ataque envía el archivo de contraseñas a la máquina del atacante (o cualquier otra víctima), donde se podrán descifrar las contraseñas.

Sistemas afectados
Diversos sistemas UNIX y Linux.

Registro CVE:
CVE-1999-0047, CVE-1999-0130, CVE-1999-0131, CVE-1999-0203, CVE-1999-0204, CVE-1999-0206.

CVE-1999-0130 sólo puede utilizarse localmente.

Consejos para la resolución del problema:

- Actualizar a la última versión de sendmail y/o implementar los parches para sendmail. Consultar http://www.cert.org/advisories/CA-97.05.sendmail.html

- No ejecutar sendmail en modalidad daemon (desactivar la opción -bd) en los sistemas que no son servidores o encaminadores de correo.

sadmind y mountd

Sadmind permite la administración remota de los sistemas Solaris, proporcionando un acceso gráfico a las tareas de administración del sistema. Mountd controla y arbitra el acceso a los volúmenes NFS en los sistemas UNIX. Existen desbordamientos de buffers en estas aplicaciones que pueden ser utilizados por atacantes para obtener el acceso a la cuenta root.

Sistemas afectados
Diversos sistemas UNIX y Linux.

Sadmind: (sólo sistemas Solaris)

Registro CVE:
sadmind - CVE-1999-0977

mountd - CVE-1999-0002.

Consejos para la resolución del problema:

- Siempre que sea posible, desactivar y/o eliminar estos servicios en las máquinas que son directamente accesibles desde Internet.

- Instalar los últimos parches:

  Parches para sistemas Solaris:
  http://sunsolve.sun.com

  Para AIX de IBM:
  http://techsupport.services.ibm.com/support/rs6000.support/downloads
  http://techsupport.services.ibm.com/rs6k/fixes.html

  Para sistemas SGI:
  http://support.sgi.com/

  Para Compaq (Digital Unix):
  http://www.compaq.com/support

- Más información en:
  http://www.cert.org/advisories/CA-99-16-sadmind.html
  http://www.cert.org/advisories/CA-98.12.mountd.html

Compartición de archivos global y compartición de información inapropiada mediante NetBIOS y los puertos 135 -> 139 en Windows NT (445 en Windows 2000); exports de NFS en Unix (puerto 2049), compartición vía web en Macintosh y Appleshare/IP en los puertos 80, 427 y 548.

Todos estos servicios permiten la compartición de archivos en redes. Cuando son configurados de forma inapropiada, pueden exponer archivos de sistema críticos o incluso permitir un acceso completo al sistema de archivos a cualquiera que esté conectado en la red. Muchos propietarios de ordenadores y administradores utilizan estos servicios para permitir que sus sistemas de archivos sean visibles (en modalidad de lectura y/o escritura) en un intento de hacer más conveniente el acceso a los datos. Los administradores de un sistema del gobierno de los EE.UU. dedicado al desarrollo de software para la planificación de misiones lo configuraron de tal forma que cualquiera pudiera leer los archivos, de forma que los compañeros de otros edificios tuvieran un fácil acceso a la información. Sólo dos días después, otras personas habían descubierto esta compartición abierta y robaron el software de planificación de misiones.

Cuando la compartición de archivos se encuentra activada en las máquinas Windows, éstas son vulnerables al robo de información y a los efectos de determinados tipos de virus de rápida difusión. Un virus recientemente publicado, denominado "911 Worm" utiliza la compartición de archivos de los sistemas Windows 95 y 98 para propagarse y hace que el ordenador infectado utilice su módem para llamar al número de emergencias (911 en EE.UU.). Los ordenadores Macintosh son también vulnerables a los ataques de la compartición de archivos.

El mismo mecanismo NetBIOS que permite la compartición de archivos en Windows puede ser utilizado para obtener información sensible de los sistemas NT. Mediante la utilización de una "sesión nula" al servicio de sesión NetBIOS, se puede obtener información sobre los usuarios y grupos (nombre de usuario, fecha de la última conexión, política de contraseñas, información de acceso remoto), información sobre el sistema y determinadas entradas del registro. Esta información es habitualmente utilizada para organizar un ataque de fuerza bruta para determinar contraseñas, o bien una simple prueba de diversas contraseñas.

Sistemas afectados:
Sistemas UNIX, Windows y Macintosh.

Registro CVE:
Comparticiones SMB con un escaso control de acceso - CAN-1999-0520
Exports de NFS para todos - CAN-1999-0554

Estos registros candidatos serán, con toda probabilidad, ampliamente modificados antes de ser aceptados como registros CVE.

Consejos para la resolución del problema:

- Cuando se comparten discos montados, verificar que únicamente los directorios necesarios son compartidos.

- Para mayor seguridad, permitir sólo la compartición a direcciones IP específicas, dado que los nombres de DNS pueden ser suplantados.

- En los sistemas Windows, verificar que todas las comparticiones están protegidas mediante contraseñas fuertes.

- En los sistemas Windows NT prevenir la enumeración anónima de usuarios, grupos, configuración del sistema y valores del registro mediante una conexión anónima.

  Bloquear las conexiones entrantes al servicio de sesión NetBIOS (puerto tcp 139) en el direccionador o en la máquina NT.

  Considerar la implantación de la clave del registro `RestrictAnonymous` en aquellos sistemas independientes o en dominios no confiables y que estén conectados a Internet:
  NT 4: http://support.microsoft.com/support/kb/articles/Q143/4/74.asp
  Windows 2000:
  http://support.microsoft.com/support/kb/articles/Q246/2/61.ASP

- En los sistemas Macintosh, deshabilitar las extensiones de compartición de archivos y compartición web si no son realmente necesarios. Si la compartición de archivos debe estar activar, verificar la utilización de contraseñas fuertes para el acceso y detener la compartición de archivos cuando no se utilice.

  Para desactivar de forma permanente la compartición web en MacOS 8 y MacOS 9, borrar los archivos y reiniciar:

  ```
  Carpeta del sistema:Paneles de control:Compartir web
  Carpeta del sistema:Extensiones:Extensión compartir web
  ```

  Para deshabilitar permanentemente AppleShare/IP en MacOS 9, borrar el siguiente archivo y reiniciar la máquina:

  ```
  Carpeta del sistema:Extensiones:Shareway IP Personal
  Subord.
  ```

- Existe un test rápido, seguro y gratuito para determinar si la compartición de archivos NetBIOS y las vulnerabilidades asociadas están presentes. Este test puede realizarse desde CUALQUIER sistema operativo y se encuentra en la página web de Gibson Research Corporation. Sólo es necesario acceder a la página http://grc.com y hacer clic en el icono "ShieldsUP" para recibir un informe, en tiempo real, de cualquier vulnerabilidad NetBIOS accesible desde Internet. Se incluyen instrucciones detalladas para ayudar a los usuarios de Microsoft Windows en la eliminación de estas vulnerabilidades.

Cuentas de usuario, especialmente la de root o del administrador sin contraseñas o con contraseñas débiles.

Existen sistemas que vienen preconfigurados con cuentas de usuario de demostración o invitado que carecen de contraseña o utilizan una contraseña por omisión ampliamente conocida. Los operarios de servicio acostumbran a dejar las cuentas creadas para el mantenimiento sin contraseñas y determinados sistemas de gestión de base de datos instalan cuentas de administración utilizando contraseñas por omisión. Por otra parte, los administradores de sistemas suelen utilizar contraseñas que son fácilmente identificables ('amor', 'dinero', 'magia' son muy habituales) o, simplemente, una contraseña en blanco. La utilización de las contraseñas por omisión permite a los atacantes el acceso a los sistemas sin ningún esfuerzo. Muchos atacantes prueban en primer lugar, antes de lanzar un ataque más sofisticado, el uso de las contraseñas por omisión y, si es necesario, a continuación con las contraseñas más habituales. Las cuentas comprometidas suponen que el atacante se encuentra dentro del cortafuegos y de la máquina objetivo. Una vez dentro, la mayoría de los atacantes utilizan algunos de los ampliamente divulgados métodos para obtener el privilegio de root o administrador.

Sistemas afectados:
Todos los sistemas.

Registro CVE:
Contraseñas de Unix fácilmente identificables (débiles) - CAN-1999-0501

Contraseñas por omisión o en blanco de Unix - CAN-1999-0502

Contraseñas de NT fácilmente identificables (débiles) - CAN-1999-0503

Contraseñas por omisión o en blanco de NT - CAN-1999-0504

Estos registros candidatos serán, con toda probabilidad, ampliamente modificados antes de ser aceptados como registros CVE.

Consejos para la resolución del problema:

- Crear una política de contraseñas aceptable donde se indique la asignación de responsabilidades y la frecuencia con que debe verificarse la calidad de las contraseñas. Asegurarse que los altos ejecutivos de la empresa no estén exentos. Igualmente, incluir en la política el requisito de modificar todas las contraseñas por omisión como paso previo a la conexión de un ordenador a Internet, especificando las penalizaciones por incumplimiento de la norma.

- **¡MUY IMPORTANTE!** Obtener autorización por escrito para verificar las contraseñas.

- Verificar la fortaleza de las contraseñas mediante programas de craqueo de contraseñas:

  Para Windows NT: l0phtcrack http://www.l0pht.com

Para UNIX: Crack http://www.users.dircon.co.uk/~crypto

- Implementar utilidades que verifiquen las contraseñas en el momento en que se crean.

  Para UNIX: Npasswd, http://www.utexas.edu/cc/unix/software/npasswd
  Para Windows NT:
  http://support.microsoft.com/support/kb/articles/Q161/9/90.asp

- Forzar la expiración periódica de las contraseñas (de acuerdo con la frecuencia indicada en la política de seguridad).

- Mantener históricos de contraseñas para evitar que los usuarios vuelvan a utilizar las contraseñas antiguas.

Para información adicional, consultar:
http://www.cert.org/tech_tips/passwd_file_protection.html
http://www.cert.org/incident_notes/IN-98.03.html
http://www.cert.org/incident_notes/IN-98.01.irix.html

Vulnerabilidades de desbordamiento de buffer o configuración incorrecta de IMAP y POP.

IMAP y POP son unos protocolos de correo remoto muy populares ya que permiten el acceso a las cuentas de correo electrónico desde las redes internas y/o externas. Las características de ”acceso abierto” de estos servicios los hace especialmente vulnerables a ataques dado que los cortafuegos habitualmente permiten el acceso a los mismos, para permitir el acceso remoto al correo electrónico. Los atacantes que explotan las vulnerabilidades en IMAP o POP habitualmente obtiene acceso instantáneo como root.

Sistemas afectados:
Diversos sistemas UNIX y Linux.

Registro CVE:
CVE-1999-0005, CVE-1999-0006, CVE-1999-0042, CVE-1999-0920, CVE-2000-0091

Consejos para la resolución del problema:

- Deshabilitar estos servicios en aquellas máquinas que no son servidores de correo.

- Utilizar las versiones más modernas con los parches más recientes.

  Para información adicional, consultar:
  http://www.cert.org/advisories/CA-98.09.imapd.html
  http://www.cert.org/advisories/CA-98.08.qpopper_vul.html
  http://www.cert.org/advisories/CA-97.09.imap_pop.html

- Algunos expertos aconsejan igualmente controlar el acceso a estos servicios utilizando TCP wrappers y canales encriptados tales como SSH y SSL, con el objetivo de proteger las contraseñas.

Nombres de comunidad SNMP por omisión como ‘public’ y ‘private’.

El protocolo simple de gestión de red (SNMP) es habitualmente utilizado por los administradores de red para la monitorización y administración de todo tipo de dispositivos conectados a la red, desde encaminadores hasta impresoras pasando por ordenadores. SNMP utiliza, como único mecanismo de autenticación, un ”nombre de comunidad” que se envía sin encriptar. Si la falta de encriptación ya de por si es mala, peor aún es que la mayor parte de los dispositivos SNMP utilizan como comunidad por omisión la palabra ”public”; algunos fabricantes 'inteligentes' de dispositivos de red han cambiado el nombre y utilizan la palabra ”private”.

Los atacantes pueden utilizar esta vulnerabilidad del SNMP para reconfigurar o detener, de forma remota, los dispositivos. La captura del tráfico SNMP, por otra parte, puede revelar una gran cantidad de información sobre la estructura de la red así como de los dispositivos y sistemas conectados a la misma. Esta información es muy útil para los atacantes, en vistas a la selección de blancos para sus ataques.

Sistemas afectados
Todos los sistemas y dispositivos de red.

Registro CVE:
Nombre de comunidad (public) SNMP en blanco o por omisión - CAN-1999-0517

Nombre de comunidad SNMP fácilmente identificable - CAN-1999-0516

Nombres de comunidad SNMP ocultos - CAN-1999-0254, CAN-1999-0186

Estos registros candidatos serán, con toda probabilidad, ampliamente modificados antes de ser aceptados como registros CVE.

Consejos para la resolución del problema:

- Si no se utiliza SNMP, deshabilitarlo.
- Si se utiliza SNMP, utilizar la misma política utilizada para las contraseñas, descrita en el punto 8, para los nombres de comunidad.
- Validar y verificar los nombres de comunidad mediante snmpwalk.
- Siempre que sea posible, configurar los MIBs en modalidad de sólo lectura.

Información adicional:
http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/snmp.htm#xtocid210315

Un punto de alta prioridad para usuarios y administradores de Windows: Varios agujeros de script en Internet Explorer y Microsoft Office 2000

Los recientes ataques de virus han puesto de relieve como unas macros o scripts pueden propagarse fácilmente a través de archivos asociados al correo electrónico, llegando a tener que aconsejar a los usuarios que no abran ningún archivo asociado a un mensaje que sea potencialmente peligroso. No obstante, los usuarios de Windows pueden ayudar a la propagación de peligrosos virus sin tener que abrir ningún archivo. Microsoft Outlook y Outlook Express ejecutan, en sus configuraciones por omisión, el código HTML y los scripts incluidos en los mensajes. Adicionalmente, algunos componentes ActiveX pueden ser utilizadas desde el código incluido en algunos mensajes con HTML. Algunos de los controles vulnerables son el Scriplet.typlib (incluido en IE 4.x Y 5.x) y el control UA (Office 2000). Otras posibles vulnerabilidades por la utilización de Active Scripting son la posibilidad de que un mensaje instale un programa en el ordenador del usuario.

Actualmente existe un virus, relativamente benigno, denominado KAK que se propaga utilizando estos mecanismos. En cualquier momento es posible que aparezca una versión maligna de kak. Aconsejamos que todos los usuarios y administradores configuren Outlook y Outlook Express para utilizar el correo electrónico como ”Zona de sitios restringidos” y, adicionalmente, deshabilitar todas las opciones relacionadas con Active Scripting y ActiveX dentro de esa zona. Esto se hace a través del apartado Herramientas | Opciones | Seguridad, pero puede automatizarse a través de las políticas del sistema. Microsoft ha publicado parches para los problemas individuales y está ultimando un parche que fijará los valores de seguridad en Outlook, aunque aparentemente no hay planes de arreglar Outlook Express.

Sistemas afectados:
Todos los sistemas Windows con Internet Explorer 4.x y 5.x (incluso si no se utiliza) o Office 2000. Windows 2000 no se ve afectado por algunas de las vulnerabilidades de Internet Explorer.

Registro CVE:
CVE-1999-0668
CAN-2000-0329

Consejos para la resolución del problema:
http://www.microsoft.com/security/bulletins/ms99-032.asp
http://www.microsoft.com/security/bulletins/MS99-048.asp
http://www.microsoft.com/technet/security/bulletin/MS00-034.asp

Los parches para las vulnerabilidades particulares descritas se encuentran en:
http://www.microsoft.com/msdownload/iebuild/scriptlet/en/scriptlet.htm
http://www.microsoft.com/msdownload/iebuild/ascontrol/en/ascontrol.htm
http://officeupdate.microsoft.com/info/ocx.htm

Deberá modificarse la zona de seguridad a ”sitios restringidos”, deshabilitando

todo el contenido activo en dicha zona y aplicar el parche para Outlook tan pronto como esté disponible en:

http://www.officeupdate.com/2000/articles/out2ksecarticle.htm

La actualización del sistema de detección de virus, si bien es importante, no es una solución completa a este problema. Es necesario, también, la corrección de las vulnerabilidades del software de Microsoft.

Protección perimetral para una línea adicional de defensa.

En esta sección, listamos los puertos que son habitualmente sondeados y atacados. El bloqueo de estos puertos se considera un requisito mínimo para la seguridad perimetral, aunque no debe considerarse como una lista de especificaciones completa para el cortafuegos. Una norma mucho mejor es bloquear todos los puertos que no se utilicen. E incluso sabiendo que estos puertos están bloqueados, deberemos monitorizarlos activamente para detectar intentos de intrusión. De todas formas, se hace necesario un aviso. El bloqueo de algunos de los puertos incluidos en la lista puede deshabilitar algunos servicios necesarios. Por tanto deben considerarse los efectos potenciales de estas recomendaciones de forma previa a su implementación.

1. Bloquear las direcciones suplantadas --paquetes provenientes del exterior con una dirección de origen dentro del rango de direcciones internas o privadas (RFC1918 y red 127) así como los rangos de direcciones reservados por la IANA. Bloquear, igualmente, los paquetes de direccionamiento en origen.

2. Servicios de conexión -- telnet (23/tcp), SSH (22/tcp), FTP 21/tcp), NetBIOS (139/tcp), rlogin, etc... (del 512/tcp al 514/tcp)

3. RPC y NFS-- Portmap/rpcbind (111/tcp y 111/udp), NFS (2049/tcp y 2049/udp), lockd (4045/tcp y 4045/udp)

4. NetBIOS en Windows NT -- 135 (tcp y udp), 137 (udp), 138 (udp), 139 (tcp). Windows 2000 – los puertos anteriores y también el 445 (tcp y udp)

5. X Windows -- puertos tcp del 6000 al 6255

6. Servicios de nombres -- DNS (53/udp) en todas las máquinas que no sean servidores de DNS, transferencias de zona de DNS (53/tcp) excepto en los servidores secundarios externos, LDAP (389/tcp y 389/udp)

7. Correo -- SMTP (25/tcp) en todas las máquinas excepto en los servidores de correo visibles desde el exterior; POP (109/tcp y 110/tcp), IMAP (143/tcp)

8. Web-- HTTP (80/tcp) y SSL (443/tcp) excepto en los servidores web accesibles desde el exterior; deberían bloquearse igualmente los puertos no privilegiados habitualmente utilizados por los servidores web (8000/tcp, 8080/tcp, 8888/tcp, etc.)

9. "Small Services"-- puertos inferiores al 20/tcp y 20/udp, time (37/tcp y 37/udp)

10. Miscelánea -- TFTP (69/udp), finger (79/tcp), NNTP (119/tcp), NTP (123/tcp), LPD (515/tcp), syslog (514/udp), SNMP (161/tcp y 161/udp, 162/tcp y 162/udp), BGP (179/tcp), SOCKS (1080/tcp)

11. ICMP --bloquear las solicitudes de eco entrantes (ping y traceroute) así como las solicitudes salientes de eco, tiempo excedido y no accesible **excepto** los mensajes de "paquete muy grande" (tipo 3, código 4). Esta limitación asume que deseamos privarnos de los usos legítimos del protocolo ICMP en vistas a impedir su utilización de forma maliciosa.

Información de soporte de los distribuidores de Unix

Compaq (Digital Unix)

http://www.compaq.com/support

FreeBSD

http://www.freebsd.org/security

HP-UX de HP

En Estados Unidos, Canadá, Asia-Pacífico y América del Sur:
http://us-support.external.hp.com

En Europa:
http://europe-support.external.hp.com

Seleccionar los paquetes individuales y a continuación conectar --o crear un nuevo ID de conexión.

Para obtener la matriz de parche de seguridad:
ftp://us-ffs.external.hp.com/export/patches/hp-ux_patch_matrix/

AIX de IBM

http://techsupport.services.ibm.com/rs6000.support/downloads
http://techsupport.services.ibm.com/rs6k/fixes.html

SCO (OpenServer y UnixWare)

http://www.sco.com/security
(Boletines de seguridad y parches).

http://www.sco.com/support/ftplists/index.html
(Parches generales del sistema operativo).

Sun Solaris

http://sunsolve.sun.com
(Parches y recomendaciones de seguridad).

SGI

http://support.sgi.com

Linux

Caldera
http://www.caldera.com/support/security

Debian
http://www.debian.org/security/index.en.html

Mandrake
http://www.linux-mandrake.com/en/fupdates.php3

Red Hat
http://www.redhat.com/support/updates.html

SuSE
http://www.suse.com/support/download/updates/index.html
http://www.suse.de/en/support/security/index.html

Firmantes.

- Randy Marchany, Virginia Tech
- Scott Conti, universidad de Massachusetts
- Matt Bishop, universidad de California, Davis
- Sten Drescher, Tivoli Systems
- Lance Spitzner, Sun Microsystems GESS Security Team
- Alan Paller, SANS Institute
- Stephen Northcutt, SANS Institute
- Eric Cole, SANS Institute
- Gene Spafford, CERIAS de la universidad Purdue
- Jim Ransome, Pilot Network Services
- Frank Swift, Pilot Network Services
- Jim Magdych, Network Associates, Inc.
- Jimmy Kuo, Network Associates, Inc.
- Igor Gashinsky, NetSec, Inc.
- Greg Shipley, Neohapsis
- Tony Sager, Agencia Nacional de Seguridad
- Larry Merritt, Agencia Nacional de Seguridad
- Bill Hill, MITRE
- Steve Christey, MITRE
- Viriya Upatising, Loxley Information Services Co.
- Marcus Sachs, JTF-CND, Departamento de defensa de los EE.UU.
- Billy Austin, Intrusion.com
- Christopher W. Klaus, Internet Security Systems
- Wayne Stenson, Honeywell
- Martin Roesch, Hiverworld, Inc.
- Jeff Stutzman, Healthcare ISAC
- Ed Skoudis, Global Integrity
- Gene Schultz, Global Integrity
- Kelly Cooper, Genuity
- Eric Schultze, Foundstone
- Bill Hancock, Exodus Communications
- Ron Nguyen, Ernst & Young
- Lee Brotzman, NASIRC, Allied Technology Group, Inc.
- Scott Lawler, Cert del Departamento de defensa de los EE.UU.
- Hal Pomeranz, Deer Run Associates
- Chris Brenton, Dartmouth Institute for Security Studies
- Bruce Schneier, Counterpane Internet Security, Inc.
- Nick FitzGerald, Computer Virus Consulting Ltd.
- Shawn Hernan, CERT Coordination Center
- Kathy Fithen, CERT Coordination Center
- Derek Simmel, Carnegie Mellon University
- Jesper Johansson, Boston University
- Dave Mann, BindView
- Rob Clyde, Axent
- David Nolan, Arch Paging
- Mudge, @stake

Expertos en seguridad que colaboran en la detección y solución de estas vulnerabilidades

- Robert Harris
- Scott Craig Kmart