Mejorando la seguridad Windows a través de la comprensión de las vulnerabilidades MSRPC

En los últimos dos años se han publicado un cierto número de vulnerabilidades críticas que afectan al subsistema MSRPC (RPC de Windows). Un conjunto de éstas ha sido –y sigue siendo–, aprovechado de forma masiva por gusanos y virus para comprometer sistemas Windows no parcheados. Aunque se introdujeron mejoras significativas al subsistema MSRPC en Windows XP SP2 y Windows Server 2003 SP1, los sistemas antiguos, entre los que se encuentran Windows 2000 y Windows NT 4.0, no se han beneficiado de estas mejoras. Conocer cómo se descubren y explotan las vulnerabilidades en MSRPC puede ayudar a los administradores de sistemas Windows a 'securizar' sus sistemas de forma proactiva para protegerse contra futuras vulnerabilidades y reducir, así, su riesgo.

Jean-Baptiste Marchand

MSRPC es el nombre de la implementación de Microsoft del estándar DCE-RPC (llamada a procedimiento remoto) y es un componente esencial del sistema operativo Microsoft Windows. Es lo que el sistema operativo utiliza cuando, por ejemplo, gestiona tanto el sistema local como otros sistemas Windows de forma remota.

El MSRPC es un componente clave de los dominios Windows. El tráfico de red de entornos Directorio Activo incluye un porcentaje importante de tráfico MSRPC **[1]** y es una de las razones por las que este subsistema está habilitado por omisión en todos los sistemas Windows. También se utiliza como protocolo de transporte para MAPI, el protocolo utilizado por Microsoft Exchange y por DCOM, la versión distribuida del COM de Microsoft, empleada intensivamente en las herramientas de administración de sistemas de Microsoft. En realidad, cualquier usuario de sistemas Windows utiliza MSRPC, muchas veces sin saberlo.

Cuando Microsoft corrigió una vulnerabilidad critica en una interfaz MSRPC en julio de 2003 y, tres semanas después, la aprovechó el gusano Blaster para lograr una propagación e impacto elevadísimo los administradores de sistemas Windows se dieron cuenta de que el subsistema MSRPC podría ser un vector de ataque muy peligroso.

Microsoft ha corregido desde enero de 2003 diversas vulnerabilidades en el subsistema publicando dieciseis boletines de seguridad. Esto hace evidente la importancia de entender cómo el código malicioso puede aprovechar esas vulnerabilidades y cómo deben protegerse los sistemas contra ellas.

El MSRPC se puede utilizar localmente o de forma remota, mediante la conexión a una interfaz que proporciona el acceso a las operaciones que pueden realizarse a través de ésta. Muchos componentes de Windows ejecutan servidores RPC y dan acceso a distintas interfaces **[2]**. Cada interfaz no es más que una lista de funciones que se pueden invocar en un servidor RPC.

Vectores de ataque MSRPC

Existen distintos vectores de transporte para que un sistema remoto utilice los servidores RPC. Los dos principales son el transporte TCP y el transporte SMB. El transporte TCP utiliza un servicio de asignación de extremos RPC sobre el puerto 135, que se utiliza para que un sistema pueda determinar qué puerto utiliza un servidor RPC ya que la asignación de este puerto es dinámica. El transporte SMB utiliza canalizadores con nombre (*named pipes*) en el recurso compartido IPC$. Los dos puertos TCP del servidor SMB son 139 y 445. (**Figura 1**)

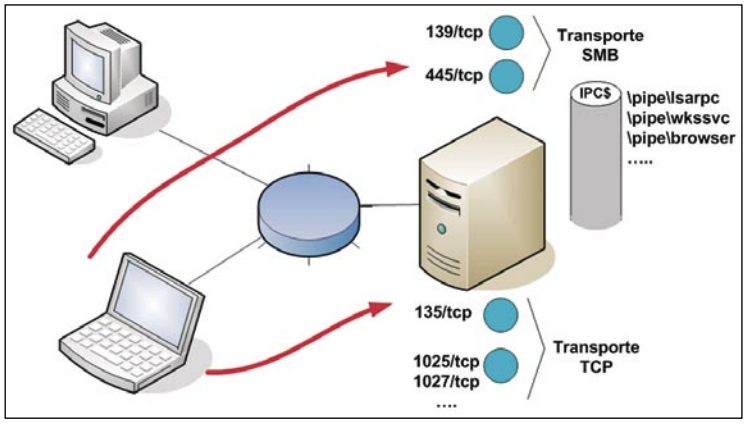

Figura 1-Vectores de ataque MSRPC

El acceso a través del transporte TCP para acceder a la mayoría de las interfaces de MSRCP no requiere de autenticación en las versiones de Microsoft Windows previas a XP SP2. Como consecuencia, un sistema remoto podría utilizar una interfaz RPC y aprovechar cualquier vulnerabilidad en ésta si el puerto 135 o bien cualquiera de los puertos dinámicos utilizados por los servidores RPC, no están convenientemente filtrados. Esto es precisamente lo que ocurrió con el puerto 135 y el gusano Blaster en agosto de 2003.

En el caso de transporte SMB, debe establecerse una sesión SMB previamente, lo que requiere normalmente de autenticación. Sin embargo, utilizando sesiones nulas (un tipo de sesión especial en el acceso SMB), es posible establecer una sesión SMB de forma anónima y acceder a algunas de las interfaces RPC. La utilización de las sesiones nulas es un problema bien conocido del protocolo SMB en Microsoft Windows pero una instalación por omisión permite su utilización, así, cualquier sistema de forma anónima, con acceso al servidor de SMB podría aprovechar también ciertas vulnerabilidades RPC. Dado que los sistemas Windows por omisión tienen varios puertos TCP abiertos, entre los que se encuentran los puertos 135, 139 y 445, esto explica por qué existen gusanos que pueden aprovechar las vulnerabilidades de MSRPC en entornos donde no hay un proceso adecuado de actualización de sistemas con parches de seguridad o un filtrado restrictivo del tráfico IP.

Investigación de vulnerabilidades MSRPC

Muchos investigadores de seguridad tienen interés en descubrir una vulnerabilidad en el MSRPC porque éste es un componente clave de todos los sistemas Microsoft Windows. Como muestra, la sección de agradecimientos de los boletines de seguridad de Microsoft relacionados con arreglos de vulnerabilidades de MSRPC suelen incluir el nombre de investigadores famosos con experiencia que descubrieron la vulnerabilidad.

Para poder investigar estas vulnerabilidades es necesario comprender en detalle la especificación de MSRPC. Se han publicado distintas herramientas y presentaciones en los últimos años que proporcionan información útil a los investigadores interesados en MSRPC. La empresa americana Immunity, por ejemplo, empezó a ofrecer un curso dedicado a la investigación de vulnerabilidades MSRPC **[3]** hace poco tiempo.

Es interesante destacar que la investigación de MSRPC empezó al final de los años 90, cuando el proyecto Samba empezó a implementar los MSRPC para hacer posible la implementación de

Boletín de seguridad Microsoft	Fecha de publicación	Interfaz RPC afectada	Aprovechamiento de forma anónima en:	Nombre del gusano	Referencia
MS03-026	16/07/03	Interfaz RPC DCOM	Windows NT, 2000, XP, 2003	Blaster	http://monkey.org/~jose/presentations/blaster-ieee.d/
MS03-039	10/09/03	Interfaz RPC DCOM	Windows NT, 2000, XP, 2003	Agobot/ Gaobot, Rbot, Sdbot, ...	http://www.microsoft.com/technet/security/bulletin/MS03-039.mspx
MS03-049	11/11/03	Interfaz RPC del servicio Workstation	Windows 2000, XP	Agobot/ Gaobot, Rbot, Sdbot, ...	http://www.eeye.com/html/research/advisories/AD20031111.html
MS04-011	13/04/04	Una interfaz RPC del servicio LSASS	Windows 2000, XP	Sasser	http://www.lurhq.com/sasser.html
MS05-039	09/08/05	Interfaz RPC del servicio Plug and Play	Windows 2000	Zotob	http://www.lurhq.com/pnpworms.html

Tabla: Gusanos que han aprovechado vulnerabilidades de MSRPC

un controlador de dominio Windows NT sobre un sistema Unix. En esa época, los miembros del proyecto descubrieron distintos problemas graves en Windows NT 4.0 que fueron posteriormente corregidos por Microsoft.

Vulnerabilidadaes MSRPC aprovechadas por código malicioso

De las dieciseis vulnerabilidades MSRPC publicadas en los dos últimos años, solo un conjunto de estas están siendo aprovechadas por los gusanos existentes. Habitualmente, cuando se publica código de ataques basándose en la vulnerabilidad se produce un proceso de actualización del código malicioso **[4]** para aprovecharla y dotarlos de capacidades adicionales para comprometer aquellos sistemas no parcheados.

Distintos tipos de código malicioso utilizan las vulnerabilidades MSRPC listadas en la tabla: MS03-026, MS03-039, MS03-049, MS04-011 y MS05-039. Un sistema infectado con uno de éstos intenta conectarse a sistemas remotos utilizando uno o más de esos puertos TCP: 135, 139, 445, así como los inmediatamente superiores al 1024 (como el 1025 y el 1026).

La misma vulnerabilidad de MSRPC puede afectar a distintas versiones de Windows pero sólo suele ser aprovechable de forma anónima sobre una versión. Por ejemplo, la reciente vulnerabilidad MS05-039 afecta a muchas versiones de Windows pero sólo puede aprovecharse de forma anónima en Windows 2000 (ver tabla).

Protección contra vulnerabilidades MSRPC

El primer paso para proteger sistemas es comprobar que se han instalado los parches que corrigen las vulnerabilidades de MSRPC.

Tanto en la configuración del sistema operativo se pueden tomar varias medidas para protegerse de forma proactiva contra futuras vulnerabilidades:

Para el transporte TCP (que utiliza el puerto 135 y puertos dinámicos): facilitar el filtrado de puertos configurando un rango fijo para los servidores RPC utilizando la herramienta rpccfg **[5] [6].**

Para el transporte SMB (puertos 139 y 445): bien desactivar el servicio Server (habitualmente sólo posible en escritorios, no en servidores) o bien restringir el uso de sesiones nulas. Son varias las medidas adicionales de bastionado a aplicar, véase **[7].**

Cabe destacar que Windows XP SP2 y Windows Server 2003 SP1 introdujeron varias mejoras para reducir el impacto de las vulnerabilidades MSRPC. En Windows XP SP2, las llamadas RPC anónimas están prohibidas por omisión excepto para el transporte SMB. En Windows Server 2003 SP1, se dispone de la misma restricción pero está deshabilitada por omisión aunque se recomienda habilitarla. En ambos casos, el transporte SMB sigue permitiendo llamadas RPC anónimas a través de sesiones nulas, por lo que es recomendable restringir éstas. Además, se puede utilizar la herramienta de cortafuego de canales con nombres de estos sistemas (como se detalla en **[8]**).

Al nivel de red también existen varias posibilidades para proteger a los sistemas:

Utilizando IPS que puedan interpretar el MSRPC y bloquear los ataques a través de este subsistema. Debido a la complejidad del protocolo, sin embargo, hay distintos métodos de evasión; sólo hay algunos fabricantes de IPS que han invertido lo suficiente en I+D como para tratar el protocolo de forma completa. El IPS Sentivist, de NFR Security, es uno de ellos (**[9]**).

Filtrando con un cortafuegos que interprete el MSRPC. Pocos lo hacen; los más conocidos son Check Point Firewall-1 y Microsoft ISA Server. El filtro MSRPC de ISA Server se utiliza sobre todo para proteger el acceso a servidores Exchange. Por su parte, Check Point Firewall-1 tiene un soporte bastante completo de MSRPC, incluyendo DCOM como se puede atestiguar analizando el código INSPECT del cortafuegos.

Por último, el analizador de red Ethereal interpreta el tráfico MSRPC de una forma muy completa. Cualquier administrador de red interesado en investigar este tipo de tráfico puede utilizar la herramienta para analizarlo y aprender más del tipo de comunicaciones que se producen en entornos Windows.

Conclusión

Debido a las múltiples vulnerabilidades publicadas en los dos últimos años es imprescindible proteger a los sistemas contra las vulnerabilidades actuales y futuras que se aprovechen del MSRPC. Además de mantener los sistemas actualizados con parches es posible utilizar varias medidas para protegerse contra futuras vulnerabilidades. Esto puede ser particularmente necesario hacerlo en los sistemas Windows más antiguos que no se pueden beneficiar de las mejoras recientes de Windows XP SP2 y Windows Server 2003 SP1 ni siquiera a través de parches. ■

Jean-Baptiste Marchand
Consultor, División de Seguridad,
GERMINUS
jbmarchand@germinus.com

Referencias

[1] *Windows network services internals*: http://www.hsc.fr/ressources/articles/win_net_srv/

[2] *Active Directory network protocols and traffic*: http://www.hsc.fr/ressources/presentations/ad_proto_traffic/

[3] *Locating Vulnerabilities in Microsoft RPC: An Offline and Runtime Reversing Approach.* http://www.immunitysec.com/education-auditingmsrpc.shtml

[4] W32/Rbot-AQF: http://www.sophos.com/virusinfo/analyses/w32rbotaqf.html

[5] *Minimizing Windows network services (Windows 2000 and Windows XP)*: http://www.hsc.fr/ressources/breves/min_srv_res_win.en.html

[6] *Minimizing Windows Server 2003 network services*: http://www.hsc.fr/ressources/breves/min_w2k3_net_srv.html

[7] *NULL sessions hardening recommendations:* http://www.hsc.fr/ressources/presentations/null_sessions/img37.html

[8] *Named pipe firewall in Windows XP SP2 and Windows Server 2003 SP1:* http://www.hsc.fr/ressources/presentations/null_sessions/img39.html

[9] *Beyond "Blaster" - MSRPC Evasions*: http://www.nfr.com/newsletter/June-05/BeyondBlaster.html