*UNAM−CERT*

*Departamento de Seguridad en Cómputo*

*DGSCA−UNAM*

---

# *Boletin de Seguridad UNAM−CERT−2007−014*

## *Buffer overflow en el RPC utilizado por el DNS de Microsoft Windows*

---

Un buffer overflow en la interface de administración de RPC (Remote Procedure Call) utilizada por el servicio DNS (Domain Name Service) de Microsoft Windows está siendo activamente explotada. Esta vulnerabiidad podría permitir a un atacante remoto ejecutar código arbitrario con privilegios de SYSTEM.

| | |
|---|---|
| **Fecha de Liberación**: | 13 de Abril de 2007 |
| **Ultima Revisión**: | 13 de Abril de 2007 |
| **Fuente**: | CERT/CC y diversos reportes de Equipos de Respuesta a Incidentes, así como foros y listas de discusión. |

**Riesgo**

Crítico

**Problema de Vulnerabilidad**

Remoto

**Tipo de Vulnerabilidad**

Ejecución Remota de Código

### I. Sistemas Afectados

- Microsoft Windows 2003 Server
- Microsoft Windows 2000 Server

### II. Descripción

La interfase de administración del RPC en el servicio de DNS de Microsoft Windows contiene un buffer overflow basado en pila. Esta vulnerabilidad puede ser activada enviando un paquete RPC creado de forma maliciosa a la interfase de administración del RPC. La interfaz de administración típicamente opera en un puerto asignado dinámicamente entre 1024/tcp and 5000/tcp.

Se debe hacer notar que esta vulnerabilidad no puede ser explotada a través del servicio de resolución de nombres de DNS (53/udp).

Más información sobre esta vulnerabilidad está disponible en la Nota de Vulnerabilidad VU#555920 y el Aviso de Seguridad de Microsoft (935964).

Esta vulnerabilidad está siendo activamente explotada.

## III. Impacto

Un atacante remoto podría ser capaz de ejecutar código arbitrario con privilegios de SYSTEM o causar una condición de negación de servicio.

## IV. Solución

Hasta hoy en día no existe una solución completa para esta vulnerabilidad. Hasta que una solución esté disponible, existen soluciones temporales que podrían reducir las opciones de explotación. Es importante entender que la configuración de la red y los requerimientos de servicio antes de decidir los cambios apropiados. Por ejemplo, deshabilitando la interfaz RPC del servicio de DNS podría prevenir que los administradores sean capaces de administrar remotamente un servidor DNS de Microsoft Windows. Considere esto cuando implemente las siguientes soluciones temporales:

- **Deshabilitar la interfase RCP utilizada por el servicio DNS de Windows**

  Esta solución temporal configurará el servicio de administración de DNS para que funcione solo a través de LPC (Local Procedure Call). Esto previene la explotación de la vulnerabilidad, sin embargo, esto también deshabilita la administración remota a través de RPC, la cual, es utilizada por el complemento MMC (Microsoft Management Console) de DNS.

  De acuerdo al Aviso de Seguridad de Microsoft (935964), la administración remota del RPC puede ser deshabilitada realizando los siguientes pasos:

  1. En el menú *Inicio* haga clic en *Ejecutar*, escriba *Regedit* y después presione *Entrar*.
  2. Navegue a la siguiente localidad del registro: *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DNS\Parameters*.
  3. En el menú *Edición* seleccione *Nuevo* y después haga clic en *Valor DWORD*.
  4. En el valor resaltado de *Nuevo valor #1* escriba *RpcProtocol* para el nombre del valor y presione *Entrar*.
  5. Haga doble clic en el nuevo valor creado y cambie el valor del dato a *4*.

  Alternativamente, el siguiente texto puede ser guardado como un archivo .REG e importado posteriormente:

  ```
  Windows Registry Editor Version 5.00
  ```

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DNS\Parameters]

"RpcProtocol"=dword:00000004
```

Reinicie el servicio de DNS para que el cambio tome efecto.

Más información sobre el comando *regedit.exe* está disponible en el Artículo de la Base de Conocimientos de Microsoft 82821.

- **Bloquear o restringir el acceso a los servicios de RPC**

  Esta solución temporal restringirá el acceso TCP/IP a todas las interfaces RPC, incluyendo la interfase RPC de administración de DNS vulnerable. Esta solución temporal no prevendrá la explotación de la vulnerabilidad, pero limitará las posibles fuentes de ataque. Esta solución temporal permitirá la administración remota utilizando la interfase RPC (complemento MMC de DNS) desde las redes seleccionadas.

  Bloquear el acceso al servicio RPC Endpoint Mapper (135/tcp) en los perímetros de la red. Se debe hacer notar que bloqueando el RPC en el perímetro de la red podría aún permitir a los atacantes dentro del perímetro explotar esta vulnerabilidad.

  De forma predeterminada el servicio RPC Endpoint Mapper (135/tcp) asigna puertos RPC entre 1024/tcp y 5000/tcp. Todo el tráfico no solicitado en estos puertos debería también ser bloqueado.

## V. Referencias


- Proyecto Seguridad en Windows, DSC/UNAM−CERT − <http://www.seguridad.unam.mx/windows>
- Nota de Vulnerabilidad VU#555920 − <http://www.kb.cert.org/vuls/id/555920>
- Aviso de Seguridad de Microsoft (935964) − <http://www.microsoft.com/technet/security/advisory/935964.mspx>
- Registration Info Editor (REGEDIT) Command−Line Switches − <http://support.microsoft.com/kb/82821>


---

El Departamento de Seguridad en Cómputo/UNAM−CERT agradece el apoyo en la traducción, elaboración y revisión de éste Documento a:

- Jesús Ramón Jiménez Rojas (jrojas at seguridad dot unam dot mx)

---

***UNAM−CERT***
***Equipo de Respuesta a Incidentes UNAM***
***Departamento de Seguridad en Cómputo***
***E−Mail: seguridad@seguridad.unam.mx***
***http://www.cert.org.mx***
***http://www.seguridad.unam.mx***
***ftp://ftp.seguridad.unam.mx***
***Tel: 56 22 81 69***

***Fax: 56 22 80 43***