UNAM-CERT

Departamento de Seguridad en Cómputo

DGSCA-UNAM

Boletín de Seguridad UNAM-CERT-2007-007

Buffer Overflow en el preprocesador DCE/RPC de Sourcefire Snort

Una vulnerabilidad de desbordamiento de pila (stack buffer overflow) en el preprocesador de DCE/RPC de Sourcefire Snort podría permitir a un intruso remoto, no autenticado ejecutar código arbitrario con privilegios del proceso de Snort.

Fecha de Liberación: 20 de Febrero de 2007

Última Revisión: 21 de Febrero de 2007

Fuente: CERT/CC y diversos reportes de Equipos de Respuesta a Incidentes, así como foros y listas de discusión

Sistemas Afectados

Snort ==2.6.1,
2.6.1.1,
2.6.1.2,
2.7.0 beta
1

**Sourcefire Intrusion
Sensors** ==4.1.x,
4.5.x, y
4.6x con
SEUs
anteriores
a SEU 64

**Sourcefire Intrusion
Sensors for Crossbeam** ==4.1.x,
4.5.x, y
4.6x con
SEUs
anteriores
a SEU 64

Riesgo

Alto

Problema de Vulnerabilidad

Remoto

Tipo de Vulnerabilidad

Ejecución Remota de Código

I. Descripción

Sourcefire Snort es una herramienta de software libre para la detección de intrusos ampliamente utilizada, Snort se incluye en varias distribuciones de sistemas operativos. El preprocesador DCE/RPC ensambla paquetes SBM y DCE/RPC fragmentados antes de que la información sea analizada por las reglas de Snort.

El código vulnerable no ensambla apropiadamente ciertos paquetes SMB y DCE/RPC. Un atacante podría explotar esta vulnerabilidad enviando paquetes TCP creados maliciosamente a un equipo o red que es monitoreada con Snort. El preprocesador DCE/RPC está habilitado de forma predeterminada, y el atacante no necesita completar una conexión TCP.

US-CERT esta etiquetando esta vulnerabilidad como [VU#196240](#). A esta vulnerabilidad se le ha asignado el siguiente número CVE [CVE-2006-5276](#). Información adicional esta disponible en los boletines de Sourcefire e ISS.

II. Impacto

Un atacante remoto no autenticado podría ser capaz de ejecutar código arbitrario con privilegios del preprocesador de Snort.

III. Referencias

[US-CERT Nota de vulnerabilidad VU#196240](#)

[Aviso de Sourcefire 2007-02-19](#)

[Servicio de Soporte Sourcefire](#)

[Nota de publicación de Snort Sourcefire 2.6.1.3](#)

[Sitio de descargas de Snort](#)

[Preprocesador DCE/RPC](#)

[IBM Internet Security Systems Protection Advisory](#)

[CVE-2006-5276](#)

IV. Solución

Actualización:

Snort 2.6.1.3 está disponible desde el sitio oficial de Snort. Los clientes de sourcefire deberán visitar el sitio de inicio de sesión para soporte de Sourcefire.

UNAM-CERT

Deshabilitar el preprocesador DCE/RPC:

Para deshabilitar el preprocesador DCE/RPC, comente la línea que carga el preprocesador en el archivo de configuración de Snort (generalmente /etc/snort.conf en sistemas UNIX y Linux):

```
[/etc/snort.conf]
```

```
...
```

```
#preprocessor dcerpc...
```

```
...
```

Reinicie el proceso de Snort para que los cambios tengan efecto.

Deshabilitando el preprocesador evitará que Snort ensamble paquetes SMB y DCE/RPC fragmentados. Esto podría permitir que los atacantes evadan el IDS.

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

- David Jiménez Domínguez (djimenez at correo dot seguridad dot unam dot mx)
- Ruben Aquino Luna (raquino 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