UNAM−CERT

Departamento de Seguridad en Cómputo

DGSCA−UNAM

Boletin de Seguridad UNAM−CERT−2005−015

Buffer overflow en el preprocesador de Back Orifice de Snort

El preprocesador de Back Orifice de Snort contiene un buffer overflow que podría permitir a un intruso remoto ejecutar código arbitrario en un sistema vulnerable

Fecha de Liberación:	18 de Octubre de 2005
Ultima Revisión:	19 de Octubre de 2005
Fuente:	CERT/CC y diversos reportes de Equipos de Respuesta a Incidentes, así como Foros y Listas de Discusión

Sistemas Afectados

Snort	>=2.4.0
Snort	<=2.4.2
Sourcefire Intrusion Sensors	==Todas

Problema de Vulnerabilidad

Remoto

Tipo de Vulnerabilidad

Buffer Overflow

I. **Descripción**

Snort es un sistema detector de intrusos (IDS por sus siglas en ingles) de software libre muy utilizado. Snort y varios de sus componentes son utilizados en otros productos IDS, sensores de intrusión de Sourcefire, además de que Snort es incluido en varias distribuciones de sistemas operativos.

Los preprocesadores de Snort son módulos que extienden su funcionalidad; analizando los paquetes antes de que el motor de detección sea ejecutado. El preprocesador para Back Orifice decodifica los paquetes para determinar si

contienen mensajes de ping de Back Orifice. El detector del código no limita adecuadamente la cantidad de datos que son leídos desde el paquete a un buffer de tamaño fijo, creando una falla potencial para un buffer overflow.

El código vulnerable procesará cualquier paquete UDP que no es originado o enviado desde el puerto predeterminado de Back Orifice (31337/udp). Un atacante podría explotar esta vulnerabilidad enviando un paquete UDP creado maliciosamente al equipo o red que es monitoreada por Snort.

UNAM−CERT ha registrado esta vulnerabilidad como UNAM−CERT−2005−492. Más información está disponible en la alerta publicada por Internet Security Systems (ISS).

II. Impacto

Un atacante remoto que pueda enviar paquetes UDP al sensor de Snort podría ejecutar código arbitrario. Snort se ejecuta comúnmente con permisos de root o SYSTEM, de maque que un intruso podría tomar control total del sistema vulnerable. El atacante no necesita dirigir el ataque a un sensor es especifico; el intruso puede dirigir el ataque a cualquier equipo o red monitoreada por Snort.

III. Solución

Actualizar

Sourcefire ha liberado Snort 2.4.3 que está disponible en el sitio de descargas de Snort. Para información de otros fabricantes, favor de referirse a la sección de Sistemas Afectados del UNAM−CERT−2005−492..

Inhabilitar el pre−procesador de Back Orifice

Para inhabilitar el pre−procesador de Back Orifice, comentar la línea que carga el pre−procesador en el archivo de configuración de Snort (usualmente /etc/snort.conf en sistemas UNIX y Linux):

```
[/etc/snort.conf]
...
#preprocessor bo
...
```

Reiniciar Snort para que los cambios surtan efecto.

Restringir el tráfico de salida

Considerar el bloqueo a los sensores de Snort de iniciar conexiones hacia afuera y restringir el tráfico hacia el exterior solamente a los hosts y redes que tienen requerimientos auténticos de comunicación con los sensores. Aunque esto no previene la explotación de la vulnerabilidad, hará más difícil el acceso del atacante a los sistemas comprometidos o el reconocimiento de otros sistemas.

IV. Apéndice A. Referencias

- US−CERT Nota de vulnerabilidad VU#175500 − <http://www.kb.cert.org/vuls/id/177500>

- Soluciones e instrucciones para mitigar disponibles para la vulnerabilidad de Snort Back Orifice − <http://www.snort.org/pub−bin/snortnews.cgi#99>
- Descargas de Snort − <http://www.snort.org/dl/>
- Snort 2.4.3 Changelog − <http://www.snort.org/docs/change_logs/2.4.3/Changelog.txt>
- Pre−procesadores − <http://www.snort.org/docs/snort_htmanuals/htmanual_2.4/node11.html#SECTION00310000000000000000>
- Ejecución de código remoto en el parsing de Back Orifice de Snort <http://xforce.iss.net/xforce/alerts/id/207>

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

- 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