Uso de Cisco Secure IDS/NetRanger Custom String Match Signatures en caso de desbordamiento del búfer remoto ocasionado por el gusano "Código rojo" en Microsoft Index Server ISAPI Extension en IIS 4.0 y 5.0

Contenido

Introducción
prerrequisitos
Requisitos
Componentes Utilizados
Convenciones
Firmas de coincidencia de cadena personalizada
Firma 1 — Acceso al servidor de interacción con intento de explotación
Firma 2 — Gusano del “Código rojo” del Desbordamiento de búfer de acceso a servidor índice
Información Relacionada

Introducción

A fines de julio de 2003, Computer Economics (una empresa de investigación independiente de Carlsbad, CA) estimó que el costo incurrido por las empresas para reparar los daños producidos a la red y la pérdida de productividad provocados por el gusano “Code Red” ascendía a $1200 millones de dólares estadounidenses. Esta estimación subió perceptiblemente con la versión posterior del gusano más potente del “código rojo II”. El Sistema de seguridad de detección de intrusos de Cisco (IDS), un componente clave del plano SAFE de Cisco, ha demostrado su valor a la hora de detectar y mitigar riesgos de seguridad de la red, entre ellos el gusano “Code Red”.

Este documento describe una actualización de software para detectar el método de explotación utilizado por el gusano “Código rojo” (vea Firma 2 abajo).

Usted puede crear las firmas de coincidencia de cadena personalizada mostradas abajo para coger la explotación de un desbordamiento de búfer para los servidores Web que ejecutan el Microsoft Windows NT y los Servicios de Internet Information Server (IIS) 4.0 o el Windows 2000 y IIS 5.0. Además, observe que el servicio de indexación en Windows XP beta también es vulnerable. El Security Advisory que describe esta vulnerabilidad está en http://www.eeye.com/html/Research/Advisories/AD20010618.html . Microsoft ha liberado una corrección para esta vulnerabilidad que se puede descargar de http://www.microsoft.com/technet/security/bulletin/MS01-033.mspx .

Las firmas discutidas en este documento estaban disponibles en la versión de la actualización de firma S(5). El Cisco Systems recomienda que los sensores estén actualizados a 2.2.1.8 o a la

actualización de firma 2.5(1)S3 antes de implementar esta firma. Los usuarios registrados pueden descargar estas actualizaciones de firma del centro del Software de Cisco Secure. Todos los usuarios pueden contactarse con el Soporte técnico de Cisco por correo electrónico y por teléfono a través de los contactos mundiales de Cisco.

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software:'

- Microsoft Windows NT y IIS 4.0
- Microsoft Windows 2000 y IIS 5.0

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Firmas de coincidencia de cadena personalizada

Hay dos firmas de coincidencia de cadena personalizada específicas para abordar este problema. Cada firma es descrita más abajo, y se proporcionan las configuraciones del producto aplicables.

Firma 1 — Acceso al servidor de interacción con intento de explotación

Esta firma activa un intento de desbordamiento de la memoria intermedia en la extensión ISAPI del servidor de índices combinado con un intento de pasar un código shell al servidor para obtener acceso privilegiado en la forma original del código. La firma sólo se activa para intentar pasar el código shell al servicio objetivo y obtener acceso total al nivel del SISTEMA. Un problema posible es que esta firma no dispara si el atacante no intenta pasar algún código shell, pero sólo ejecuta el desbordamiento de la memoria intermedia contra el servicio en un intento de bloquear el IIS y crear un rechazo del servicio.

String (cadena)

```
[Gg][Ee][Tt].*[.][Ii][Dd][Aa][\x00-\x7f]+[\x80-\xff]
```

Configuraciones del producto

- Eventos: 1

- Puerto: 80

Nota: Si cuenta con servidores Web que escucha en otros puertos TCP (por ejemplo 8080), necesita crear una coincidencia de cadena personalizada para cada número de puerto.

- Nivel de gravedad de alarma recomendado:Alto (Cisco Secure Policy Manager)5 (UNIX Director)
- Dirección:A

Firma 2 — Gusano del "Código rojo" del Desbordamiento de búfer de acceso a servidor índice

Los segundos fuegos de la firma en un desbordamiento de búfer frustrado en la Indexación de extensión ISAPI del servidor combinada con una tentativa de pasar el código del shell al servidor para tener el acceso privilegiado en la forma ofuscada que el gusano del "Código rojo" utiliza. Esta firma enciende solamente en la tentativa de pasar el código del shell al servicio de destino en un intento por tener el acceso a nivel sistema completo. Un problema posible es que esta firma no dispara si el atacante no intenta pasar algún código shell, pero sólo ejecuta el desbordamiento de la memoria intermedia contra el servicio en un intento de bloquear el IIS y crear un rechazo del servicio.

String (cadena)

```
[/]default[.]ida[?][a-zA-Z0-9]+%u
```

Nota: No hay espacios en blanco en la cadena antedicha.

Configuraciones del producto

- Eventos: 1
- Puerto: 80

Nota: Si cuenta con servidores Web que escucha en otros puertos TCP (por ejemplo 8080), necesita crear una coincidencia de cadena personalizada para cada número de puerto.

- Nivel de gravedad de alarma recomendado:Alto (Cisco Secure Policy Manager)5 (UNIX Director)
- Dirección:A

Para más información sobre el Cisco Secure IDS, refiera al Cisco Secure Intrusion Detection.

Información Relacionada

- Soporte Técnico - Routers
- Asesoría en seguridad de Cisco
- Página de soporte de Cisco Secure Intrusion Detection
- Soporte Técnico - Cisco Systems