Cómo responde Cisco Secure IDS al virus Nimba

Contenido

Introducción

Este documento explica cómo el Sistema Seguro de Detección de Intrusos (IDS) de Cisco identifica y previene ataques del gusano Nimda (también conocido como el Virus de Concepto contra el servidor Web). El complejo funcionamiento técnico del gusano está fuera del alcance de este boletín y se encuentra documentado en otros materiales. Una de las mejores descripciones técnicas del gusano NIMDA se puede encontrar en el gusano NIMDA consultivo CA-2001-26 CERT® .

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

Convenciones

Para obtener más información sobre las convenciones del documento, consulte las Convenciones de Consejos Técnicos de Cisco.

Antecedentes

El gusano NIMDA es un gusano y un virus híbridos que se está separando agresivamente en Internet. Para entender el Nimda y las capacidades del Cisco IDS de atenuar su extensión, es importante definir estos dos términos:

- Gusano: se refiere a un código maligno que se propaga automáticamente sin intervención humana.
- **El virus** refiere al código malicioso que se separa con algún tipo de intervención humana, por ejemplo cuando usted abre un email, hojea un sitio web infectado, o ejecuta manualmente un archivo infectado.

El gusano NIMDA es realmente un híbrido que exhibe las características de un gusano y de un virus. Nimda infecta de múltiples maneras, la mayoría de las cuales requieren de la intervención humana. Métodos de infección tipos gusano de los bloques de sensor del host del Cisco IDS que se separaron con las vulnerabilidades en el Internet Information Server de Microsoft (IIS). El Cisco IDS no bloquea el de tipo virus, los métodos de infección manual, por ejemplo cuando usted abre un correo electrónico, hojea un sitio web infectado, o ejecute manualmente un archivo infectado.

Cisco IDS Host Sensor brinda protección contra Nimda

El sensor del host del Cisco IDS previene los ataques del repaso de ejecución de directorio, que incluyen ésos usados por el gusano NIMDA. Cuando el gusano intenta comprometer a un servidor Web IDS-protegido Cisco, el ataque falla y el servidor no se compromete.

Estas reglas del sensor del host del Cisco IDS previenen el éxito del gusano NIMDA:

- Repaso de ejecución de directorio IIS (cuatro reglas)
- Salto de directorio IIS y Ejecución de código (cuatro reglas)
- Salto de directorio IIS con doble codificación hexadecimal (cuatro reglas)

El sensor del host del Cisco IDS también defiende contra los cambios no autorizados al contenido de la Web, así que no permite que el gusano altere las páginas web para separarse a otros servidores.

Cisco IDS cumple con las mejores prácticas de seguridad estándar para proteger los servidores Web contra Nimda. Estas mejores prácticas dictan para no leer el email o para hojear la red de un servidor Web de la producción, así como no tener recursos compartidos de red ábrase en un servidor. El sensor del host del Cisco IDS evita que comprometan al servidor Web con los exploits HTTP y IIS. Las mejores prácticas ya mencionadas se aseguran de que el gusano NIMDA no llegue en el servidor Web por algunos métodos manuales.

El sensor de red IDS de Cisco identifica al virus Nimda

El sensor de la red del Cisco IDS identifica los ataques de aplicación Web, que incluyen ésos usados por el gusano NIMDA. El sensor de la red puede identificar los ataques y proporcionar los detalles sobre el afectado o a los host comprometidos para aislar la infección con el virus Nimda.

Fuego de estas alarmas del sensor de la red del Cisco IDS:

- Acceso del WinNT cmd.exe WWW (SigID 5081)

- El doble IIS CGI decodifica (SigID 5124)
- Ataque Unicode WWW IIS (SigID 5114)
- Ataque de ejecución punto a punto de IIS (ID de señalización 3215)
- Ataque de ejecución punto a punto de IIS (ID de señalización 3216)

Los operadores no ven una alarma que identifique el Nimda por nombre. Ven una serie de las alarmas conocidas como exploits de los intentos del Nimda diversos para comprometer la blanco. Las alarmas identifican a la dirección de origen de los host se han comprometido que y que deben ser aislados de la red, ser limpiados, y ser parcheados.

Cursos de acción recomendados

Siga los siguientes pasos para proteger contra el gusano NIMDA:

1. Aplique las últimas actualizaciones para el Microsoft Outlook, Outlook Express, el Internet Explorer, y IIS disponible desde Microsoft .
2. Actualice su software de escaneo de virus con el último parche para mitigar el esparcimiento del virus.**Nota:** Usted puede descargar la última parche de virus para proteger su PC contra la infección. Si su PC se ha infectado ya, esta parche de virus permite que usted analice manualmente la unidad de disco duro de su PC y que limpie la infección de la máquina.
3. Despliegue el Cisco IDS para atenuar la amenaza, contenga la infección, y proteja los servidores.

Información Relacionada

- Cómo proteger su red del virus Nimda
- Avisos y asesoría en seguridad de productos de Cisco
- Página de soporte de Cisco Secure Intrusion Detection
- Soporte Técnico - Cisco Systems