Procedimientos de recuperación de catástrofe de emergencia de Código rojo II para una red AVVID

Contenido

Introducción

Este documento trata los procedimientos para eliminar inmediatamente la mayoría de los efectos colaterales en Cisco CallManager debido a una infección de Código rojo II generalizada además de soluciones a corto y largo plazo para asegurar y proteger mejor una red AVVID de problemas de esta naturaleza en el futuro.

prerrequisitos

Requisitos

Quienes lean este documento deben tener conocimiento de los siguientes temas:

- Administración del CallManager de Cisco
- Procedimiento de recuperación de desastre de emergencia

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco CallManager 3.x
- Microsoft Windows 2000
- Todas las versiones de Cisco Unity

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

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

Acciones inmediatas

Complete estos pasos:

1. Funcione con la última triunfo-OS-actualización (disponible en la sección crypto de la página apropiada de la descarga de la Versión de Callmanager en el CCO) en todos los servidores de la Telefonía IP que funcionan con el Windows 2000, y funcione con la utilidad de reparación apropiada (Microsoft tiene una herramienta disponible) y/o (disponible desde McAfee) cierre manualmente las entradas posteriores creadas por el código rojo II. Para los servidores de IP Telephony que funcionan con NT4.0 IIS, instale el Service Pack 6a y luego, la corrección del Código Rojo.**Precaución:** Como este gusano crea entradas posteriores, si el servidor estaba conectado directamente a Internet y alguien puede haber colocado más entradas posteriores en él mientras estaba comprometido, o si existe la posibilidad de que el servidor esté más comprometido desde dentro de la red, la acción más segura sería hacer una copia de seguridad de los datos y reinstalar el servidor desde cero.
2. Pare y inhabilite el Servicio de administración de IIS y el servicio editorial de Internet en todos los suscriptores del Cisco CallManager, y cualquier servidor que no los requiera. Estos servicios deben permanecer activos en el CallManager Publisher de Cisco.Para ejecutar esta tarea, siga estos pasos:Traiga para arriba a servicios el applet yendo al **Start (Inicio) > Programs (Programas) > Administrative Tools (Herramientas administrativas) > Services (Servicios)**.Haga clic derecho en Servicio de administración IIS y seleccione Detener. Esto también para el servicio editorial de Internet.**Servicio de administración de IIS del** click derecho y **propiedades** selectas. Cambie el tipo de inicialización para desactivar y luego, cierre la ventana.Haga clic con el botón derecho del ratón el **World Wide Web que publica** y seleccione las **propiedades**. Cambie el tipo de inicialización para desactivar y luego, cierre la ventana.
3. Repare todos los servidores IIS conocidos en la red.
4. Implemente cargas telefónicas actualizadas.Para los sistemas del Cisco CallManager 3.0x, descarga ciscocm_3-0-11_spA.exe del cisco.com. De la página del ccmadmin vaya al **System (Sistema) > Device Defaults (Valores predeterminados del dispositivo)** y fije las cargas del dispositivo de 7940/7960 al **P003E310**. Haga clic en **Update** (Actualizar).Para los sistemas de Cisco CallManager 3.1x, descargue ciscocm_3-1-1_spA.exe desde Cisco.com. De la página del ccmadmin vaya al **System (Sistema) > Device Defaults (Valores predeterminados del dispositivo)** y fije las cargas del dispositivo de 7940/7960 al **P00303010100**. Haga clic en **Update** (Actualizar).Para ambo 3.0 y 3.1 del Cisco CallManager, vaya al **sistema > al grupo de CallManager**. Seleccione el primer grupo en el lado izquierdo haga clic en Reset Devices (Reiniciar dispositivos) y cuando, cuando se le pida, seleccione OK. Realice esto para cada grupo de Cisco CallManagers presente para que los teléfonos obtengan sus nuevas cargas.Los sistemas 3.2x y 3.3x del Cisco

CallManager no requieren una carga actualizada del teléfono, pues incluyen todos los arreglos necesarios.

5. Identifique y tome el cuidado de los servidores IIS infectados restantes en la red (esto podría estirar fácilmente en una solución a corto plazo, dependiendo de cuántos servidores IIS rogue están en la red). Aquí se presentan dos métodos:En el servidor de publicación del Cisco CallManager, o cualquier otro servidor IIS con el registro habilitado, vaya a **c:\winnt\system32\logfiles\w3svc1** y acceda el archivo del registro más reciente. Estos archivos se nombran mediante la convención de ex000000.log.Busque una línea similar a esta:`2001-08-09 00:11:57 172.20.148.189 - 172.20.225.130 80 GET /default.ida XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XX%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090% u6858%ucbd3%u7801%u9090%u9090%u8190%u 00c3%u0003%u8b00%u531b% u53ff%u0078%u0000%u00=a200 -`En este caso, la dirección IP 172.20.148.189 es el servidor atacante. Encuentre lo y la corrección o limpíela, o desconéctela de la red.Repita este proceso hasta que se hayan localizado y reparado todos los servidores restantes infectados con código rojo.Otro método es utilizar el eEye de la utilidad gratuita disponible desde - CodeRedScanner. Esta utilidad analiza un en un momento del C de la clase que busca los equipos infectados y las máquinas vulnerables a un ataque basado .ida. el eEye tiene un escáner de la clase B disponible para un coste adicional.

Soluciones a corto plazo

- Asegúrese de que Calidad de servicio (QoS) esté configurada de manera adecuada en toda su red para dar prioridad al tráfico de voz sobre el tráfico de datos. Para ayudar a asegurarse de que la Calidad de voz está afectada lo menos posible durante el recordatorio de operaciones de limpieza, refiera a las recomendaciones proporcionadas en las soluciones de interconexión de redes de Cisco y las guías del diseño de calidad de srevicio (QoS) y las guías de diseño de la solución de telefonía de Cisco IP.
- Establezca la VLAN de voz y la de datos por separado siguiendo los recursos de las soluciones de Cisco IP Telephony. Esto podía ser una solución a largo plazo dependiendo del tamaño y de la complejidad de la red implicada.

Soluciones a largo plazo

Una vez que la emergencia inmediata ha terminado, refiera a la CAJA FUERTE: Seguridad para telefonía IP profundizado. Este documento proporciona información de mejores prácticas a los interesados en diseñar e implementar redes de IP Telephony seguras.

Información Relacionada

- Soporte de tecnología de voz
- Soporte de Productos de Voice and Unified Communications
- Troubleshooting de Cisco IP Telephony
- Soporte Técnico y Documentación - Cisco Systems