Cisco collaboration server 5.0: Resolviendo problemas la vulnerabilidad de seguridad causada por los métodos HTTP TRACE/TRACK

Contenido

Introducción

Este documento dirige los pasos para trabajar alrededor de la vulnerabilidad de seguridad causada por los métodos HTTP TRACE/TRACK para los Productos que utilizan los Servicios de Internet Information Server de Microsoft (IIS) como el web server. El Cisco collaboration server 5.0 utiliza IIS 5.0 como el web server y es susceptible a esta vulnerabilidad. La solución es utilizar la utilidad del URLScan de Microsoft para inhabilitar los métodos HTTP TRACE/TRACK.

prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Microsoft Windows 2000 Server
- Cisco collaboration server 5.0
- Microsoft IIS 5.0
- Utilidad del URLScan de Microsoft

Componentes Utilizados

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

- Microsoft Windows 2000
- Versiones 5.0 del Cisco collaboration server
- Microsoft IIS 5 (al usar el Windows 2000)
- URLScan 2.5 de Microsoft

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Vulnerabilidad del seguimiento del Cruz-sitio del soporte del método del web server HTTP TRACE/TRACK

Un web server fue detectado que soporta el método de la TRAZA HTTP. Este método permite el hacer el debug de y análisis de Seguimiento de conexión para las conexiones del cliente al web server. Por la especificación HTTP, cuando se utiliza este método, el web server produce eco detrás la información enviada a él por el cliente sin modificar y sin filtro. El web server de Microsoft IIS utiliza una PISTA del alias para este método, y es funcionalmente lo mismo.

Una vulnerabilidad relacionada con este método fue descubierta. Un malévolo, componente activo en una página web puede enviar las peticiones de la TRAZA a un web server que soporte este método de la TRAZA. Generalmente, la Seguridad del navegador rechaza el acceso a los sitios web fuera del dominio del actual sitio. Aunque sea poco probable y difícil alcanzar, sea posible, en presencia de otras vulnerabilidades del navegador, porque del contenido HTML activo hacer las peticiones del externo a los web server arbitrarios más allá del web server de recibimiento. Porque el web server elegido entonces produce eco detrás el pedido de cliente sin filtro, la respuesta también incluye (si está abierto una sesión) los credenciales de autenticación Cookie-basados o basados en web que el navegador envió automáticamente a la aplicación de Web especificada en el web server especificado. La significación de la capacidad de la TRAZA en esta vulnerabilidad es que el componente activo en la página visitada por el usuario de la víctima no tiene ningún acceso directo a esta información de autenticación, pero la recibe después de que el web server de la blanco la produzca eco detrás como respuesta de la TRAZA. Porque esta vulnerabilidad existe como soporte para un método requerido por la especificación del protocolo HTTP, la mayoría de los web server comunes son vulnerables.

Microsoft IIS: Microsoft liberó el **URLScan** (http://www.microsoft.com/windows2000/downloads/recommended/urlscan/default.asp), que se pueden utilizar para defender todos los pedidos entrantes basados en los rulesets personalizados. El URLScan se puede utilizar para esterilizar o para inhabilitar las peticiones de la TRAZA de los clientes. Observe esa PISTA de los alias IIS PARA LOCALIZAR. Por lo tanto, si el URLScan se utiliza para bloquear específicamente el método de la TRAZA, el método de la PISTA se debe también agregar al filtro. El URLScan utiliza el archivo de configuración urlscan.ini, generalmente en \System32\InetSrv\URLScandirectory.

En eso, hay dos secciones: `AllowVerbs` y `DenyVerbs`. Se utiliza el anterior si la variable de `UseAllowVerbs` se fija a **1**; si no (si está fijado a 0), se utiliza el `DenyVerbs`. Claramente, cualquiera se puede utilizar, dependiendo de si usted quiere una Valor por defecto-Negar-Explícito-permisión o una directiva de la Valor por defecto-Permitir-Explícito-negación. Para rechazar los métodos de la TRAZA y de la PISTA con el URLScan, primero quite la PISTA, LOCALICE los métodos de la sección de AllowVerbs y agreguelos a la sección de DenyVerbs. Con esto, el URLScan rechazará

todos los métodos de la TRAZA y de la PISTA, y genera una página del error para todas las peticiones usando ese método. Para habilitar los cambios, recomience el servicio editorial de Internet del elemento de los **servicios** > del **panel de control**.

Instale y configure la versión 2.5 utilitaria del URLScan para inhabilitar el método HTTP TRACE/TRACK

Complete estos pasos:

1. Instale el URLScan 2.5 en el Cisco collaboration server. Para descargar el URLScan 2.5, refiera a este sitio Web de Microsoft:http://microsoft.com/downloads/details.aspx?FamilyId=23D18937-DD7E-4613-9928-7F94EF1C902A&displaylang=en
2. Edite el archivo de propiedades urlscan.ini presente en el **servidor** <Windows2000 **instalan drive>:\WINNT\system32\inetsrv\urlscan.**
3. Cambie la propiedad de `AllowDotinPath` a partir de la 0 a 1. por abandono, el URLScan no permite los puntos en los URL, y el Cisco collaboration server requiere esta propiedad ser fijado a 1 (los agentes no podrán iniciar sesión si esta propiedad se fija a 0).
4. Agregue los métodos de la TRAZA y de la PISTA bajo sección de `DenyVerbs`, y cambie la propiedad de `AllowVerbs` a partir de la 1 a 0.
5. Recomience los servicios de la información sobre Internet Services(IIS)/del World Wide Web del elemento de los **servicios** > del **panel de control** en el Cisco collaboration server.

Información Relacionada

- Soporte Técnico y Documentación - Cisco Systems