Contenu

Introduction

Ce document adresse les étapes pour fonctionner autour de la faille de la sécurité provoquée par les méthodes du HTTP TRACE/TRACK pour les Produits qui utilisent l'Internet Information Services de Microsoft (IIS) comme web server. Le Cisco Collaboration Server 5.0 utilise IIS 5.0 comme web server et est susceptible de cette vulnérabilité. La solution est d'utiliser Microsoft ? utilitaire s URLScan pour désactiver les méthodes du HTTP TRACE/TRACK.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Microsoft Windows 2000 Server
- Cisco Collaboration Server 5.0
- Microsoft IIS 5.0
- Utilitaire de Microsoft URLScan

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Microsoft Windows 2000
- Versions 5.0 de Cisco Collaboration Server
- Microsoft IIS 5 (à l'aide du Windows 2000)
- Microsoft URLScan 2.5

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Vulnérabilité de suivi de Croix-site de support de méthode du HTTP TRACE/TRACK de web server

On a détecté un web server qui prend en charge la méthode de SUIVI de HTTP. Cette méthode permet l'analyse de suivi d'élimination des imperfections et de connexion pour des connexions du client au web server. Par spécification de HTTP, quand cette méthode est utilisée, le web server fait écho de retour les informations envoyées à lui par le client non modifié et non filtré. Le web server de Microsoft IIS utilise une PISTE de pseudonyme pour cette méthode, et est fonctionellement identique.

Une vulnérabilité liée à cette méthode a été découverte. Un composant malveillant et actif dans une page Web peut envoyer des demandes de SUIVI à un web server qui prend en charge cette méthode de SUIVI. Habituellement, la Sécurité de navigateur rejette l'accès aux sites Web en dehors de du domaine du site actuel. Bien que peu susceptible et difficile de réaliser, il soit possible, en présence d'autres vulnérabilités de navigateur, pour que le contenu actif HTML fasse des demandes externes aux web server arbitraires au delà du web server de accueil. Puisque le web server choisi fait écho alors de retour la demande de client non filtrée, la réponse inclut également (si ouvert une session) les qualifications basées sur Témoin ou basées sur le WEB d'authentification que le navigateur a automatiquement envoyées à l'application Web spécifiée sur le web server spécifié. L'importance de la capacité de SUIVI dans cette vulnérabilité est que le composant actif dans la page visitée par l'utilisateur de victime n'a aucun accès direct à ces informations d'authentification, mais ce reçoit après que le web server de cible le fasse écho de retour comme réponse de SUIVI. Puisque cette vulnérabilité existe comme soutien d'une méthode exigée par la spécification de protocole HTTP, la plupart des web server communs sont vulnérables.

Microsoft IIS : Microsoft a libéré **URLScan** (http://www.microsoft.com/windows2000/downloads/recommended/urlscan/default.asp), qui peut être utilisé pour examiner toutes les demandes en entrée basées sur les rulesets personnalisés. URLScan peut être utilisé pour assainir ou désactiver les demandes de SUIVI des clients. Notez que PISTE de pseudonymes IIS POUR TRACER. Par conséquent, si URLScan est utilisé pour bloquer spécifiquement la méthode de SUIVI, la méthode de PISTE devrait également être ajoutée au filtre. URLScan utilise le fichier de configuration urlscan.ini, habituellement dans \System32\InetSrv\URLScandirectory.

Dans cela, il y a deux sections : `AllowVerbs` et `DenyVerbs`. L'ancien est utilisé si la variable d'`UseAllowVerbs` est placée à **1** ; autrement (si réglé à 0), le `DenyVerbs` sont utilisés. Clairement, l'un ou l'autre peut être utilisé, selon si vous voulez un Par défaut-Refuser-Explicite-autoriser ou une stratégie de Par défaut-Autoriser-Explicite-refuser. Afin de rejeter des méthodes de SUIVI et de PISTE par URLScan, pour retirer d'abord la PISTE, TRACER des méthodes de l'AllowVerbs les sectionnent et ajoutent à la section de DenyVerbs. Avec ceci, URLScan rejettera toutes les méthodes de SUIVI et de PISTE, et génère une page d'erreur pour toutes les demandes suivre cette méthode. Afin d'activer les modifications, redémarrez le service d'édition de World Wide Web de l'élément de **services** > de **panneau de configuration**.

Installez et configurez la version 2.5 de service d'URLScan pour désactiver la méthode du HTTP TRACE/TRACK

Procédez comme suit :

1. Installez URLScan 2.5 dans le Cisco Collaboration Server. Afin de télécharger URLScan 2.5, référez-vous à ce site Web de Microsoft :http://microsoft.com/downloads/details.aspx?FamilyId=23D18937-DD7E-4613-9928-7F94EF1C902A&displaylang=en
2. Éditez le fichier de propriétés urlscan.ini actuel dans le **serveur** <Windows2000 **installent drive>:\WINNT\system32\inetsrv\urlscan.**
3. Changez la propriété d'`AllowDotinPath de` 0 à 1. Par défaut, URLScan ne permet pas des points dans l'URLs, et le Cisco Collaboration Server exige de cette propriété d'être placée à 1 (les agents ne pourront pas ouvrir une session si cette propriété est placée à 0).
4. Ajoutez les méthodes de SUIVI et de PISTE sous la section de `DenyVerbs`, et changez la propriété d'`AllowVerbs de` 1 à 0.
5. Redémarrez les services de données Internet Services(IIS)/World Wide Web de l'élément de **services** > de **panneau de configuration** sur le Cisco Collaboration Server.

Informations connexes

- Support et documentation techniques - Cisco Systems