Procédures Code Red II de reprise sur sinistre d'urgence pour un réseau AVVID

Contenu

Introduction

Ce document couvre les procédures pour éliminer immédiatement la plupart des effets secondaires au Cisco CallManager dû à une infection répandue du Code Red II, avec les solutions proches et à long terme mieux pour sécuriser et protéger un réseau AVVID contre des problèmes relatifs à l'avenir.

Conditions préalables

Conditions requises

Les lecteurs de ce document devraient avoir connaissance des sujets suivants :

- Gestion de Cisco CallManager
- Procédure de reprise sur sinistre d'urgence

Composants utilisés

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

- Cisco CallManager 3.x
- Microsoft Windows 2000
- Toutes les versions de Cisco Unity

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-

vous que vous comprenez l'effet potentiel de toute commande.

Conventions

Pour plus d'informations sur les conventions de documents, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Actions immédiates

Procédez comme suit :

1. Exécutez la dernière victoire-SYSTÈME D'EXPLOITATION-mise à jour (disponible dans la crypto section de la page appropriée de téléchargement de version de CallManager sur CCO) sur tous les serveurs de Téléphonie sur IP exécutant le Windows 2000, et exécutez l'utilitaire approprié de réparation (Microsoft a un outil disponible) et/ou manuellement (fourni par McAfee) clôturez les portes dérobées créées par le Code Red II. Pour des serveurs de Téléphonie sur IP exécutant NT4.0 IIS, installez le Service Pack 6a et puis la difficulté de Code Red.**Attention :** Puisque ce ver crée des portes dérobées, si le serveur était directement connecté à l'Internet et quelqu'un pourrait avoir placé plus de portes dérobées dans lui tandis qu'il était compromis, ou si la possibilité du serveur étant encore compromis de votre réseau existe, l'action la plus sûre serait sauvegarde les données et réinstallerait le à partir de zéro de serveur.
2. Arrêtez et désactivez le service d'admin IIS et le service d'édition de World Wide Web sur tous les abonnés de Cisco CallManager, et n'importe quel serveur qui n'a pas besoin de eux. Ces services doivent rester actifs sur le Cisco CallManager Publisher.Pour effectuer cette tâche, suivez ces étapes :Apportez l'applet de services en allant au **Start > Programs > Administrative Tools > Services**.**Le service d'admin du** clic droit **IIS** et sélectionnent l'**arrêt**. Ceci arrête également le service d'édition de World Wide Web.**Service d'admin du** clic droit **IIS** et **Properties** choisi. Changez le type de démarrage **pour désactiver**, et fermez la fenêtre.**Édition de World Wide Web de** clic droit et **Properties** choisi. Changez le type de démarrage **pour désactiver**, et fermez la fenêtre.
3. Corrigez ou réparez tous les serveurs connus IIS dans le réseau.
4. Deploy a mis à jour des chargements de téléphone.Pour des systèmes du Cisco CallManager 3.0x, téléchargement ciscocm_3-0-11_spA.exe de Cisco.com. De la page de CCMAdmin allez aux **par défaut de système > de périphérique** et placez les chargements de périphérique de 7940/7960 à **P003E310**. Cliquez sur **Update**.Pour des systèmes du Cisco CallManager 3.1x, téléchargement ciscocm_3-1-1_spA.exe de Cisco.com. De la page de CCMAdmin allez aux **par défaut de système > de périphérique** et placez les chargements de périphérique de 7940/7960 à **P00303010100**. Cliquez sur **Update**.Pour le Cisco CallManager 3.0 et 3.1, allez au **système > au groupe de CallManager**. Sélectionnez le premier groupe du côté gauche, et cliquez sur les **périphériques de remise**, **OK** choisi une fois incité. Faites ceci pour chaque groupe de Cisco CallManager présent pour les téléphones pour obtenir leurs nouveaux chargements.Les systèmes 3.2x et 3.3x de Cisco CallManager n'exigent pas un chargement mis à jour de téléphone, car ils incluent toutes les difficultés nécessaires.
5. Identifiez et prenez soin des autres serveurs infectés IIS sur le réseau (ceci pourrait facilement s'étendre dans une solution à court terme, selon combien de serveurs de l'escroc IIS sont sur le réseau). Voici deux méthodes :Sur le serveur de édition de Cisco

CallManager, ou n'importe quel autre serveur IIS avec le logging enabled, allez à **c:\winnt\system32\logfiles\w3svc1** et accédez au fichier journal le plus récent. Ces fichiers ont une convention nommante d'ex000000.log.Recherchez une ligne semblable à ceci :`2001-08-09 00:11:57 172.20.148.189 - 172.20.225.130 80 GET /default.ida XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX 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 -`Dans ce cas, l'adresse IP 172.20.148.189 est le serveur de attaque. Trouvez-le et corrigez-ou nettoyez-le, ou démontez-le du réseau.Répétez ce processus jusqu'à ce que tous les serveurs Rouge-infectés par code restant se soient trouvés et en considération pris.Une autre méthode est d'utiliser l'utilitaire gratuit fourni par l'eEye - CodeRedScanner. Cet utilitaire balaye un C de classe à la fois recherchant les ordinateurs infectés et les ordinateurs vulnérables à une attaque basée par .ida. l'eEye a un scanner de la classe B disponible pour des frais supplémentaires.

Solutions à court terme

- Assurez-vous que vous avez le Qualité de service (QoS) configuré correctement dans tout votre réseau pour donner la priorité au trafic vocal au-dessus du trafic de données. Pour aider à s'assurer que la Qualité vocale est affectée le moins possible pendant le reste des exécutions de nettoyage, référez-vous aux recommandations fournies dans les solutions de Cisco Networking et les guides de conception de QoS et les guides de conception de solution Cisco de téléphonie IP.
- Établissez la Voix distincte et les données VLAN, suivant les ressources en solutions de Téléphonie sur IP de Cisco. Ceci a pu être une solution à long terme selon la taille et la complexité du réseau impliqué.

Solutions à long terme

Une fois que l'urgence immédiate est terminée, référez-vous au COFFRE-FORT : Sécurité de Téléphonie sur IP en profondeur. Ce document fournit des informations de meilleure pratique aux ayants droit pour concevoir et mettre en application les réseaux sécurisés de Téléphonie sur IP.

Informations connexes

- Assistance technique concernant la technologie vocale
- Assistance concernant les produits vocaux et de communications unifiées
- Dépannage des problèmes de téléphonie IP Cisco
- Support et documentation techniques - Cisco Systems