MS Windows W32.Blaster.Worm affecte Cisco CallManager et les applications de téléphonie IP

Contenu

Introduction

La Microsoft Corporation a récemment annoncé une faille de la sécurité dans son système d'exploitation Windows, qui permet des attaques du W32.Blaster.Worm au serveur Cisco CallManager et au Cisco Conference Connection (ccc), le Cisco Emergency Responder (CER), Cisco IP Contact Center (IPCC) des applications expriment et PAs. Cette faille de la sécurité est dans une interface composante du protocole RPC du modèle objet distribuée par Windows (DCOM) (RPC).

Ce virus peut également être connu en tant que :

- W32/Lovsan.worm (NAI)
- Win32.Poza (CA)
- WORM_MSBLAST.A (tendance)

Les informations complémentaires peuvent être trouvées sur le site Web de Microsoft à ces emplacements :

- Bulletin MS03-026 de Sécurité de Microsoft
- Alerte de virus au sujet du ver W32.Blaster.Worm
- Ce que vous devriez connaître le ver blaster

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

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

- Windows 2000 Server
- Toutes les versions de Cisco CallManager
- Ccc, CER, IPCC Express, ISN, et PA

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.

Problème - Vulnérabilité RPC DCOM

Un état basé sur pile de débordement de tampon a été découvert dans l'interface RPC de Microsoft pour DCOM. C'est une principale fonction du noyau de Windows, et ne peut pas être désactivée. Puisque c'est une fonction du noyau (mise en application par l'intermédiaire de SVCHOST.EXE), les attaques réussies ont comme conséquence le privilège de système. Messages particulièrement ouvrés envoyés à l'exploit du port 135 le débordement de tampon.

Symptômes du problème

Le code d'exploit circule exécute dans la nature le code de shell après le débordement de tampon. Ceci permet l'Accès à distance à une commande shell et à un à télécommande complet et privilégié du système. Vous pourriez probablement voir un visualiseur d'erreurs en cas sur un système infecté.

Tous les ordinateurs infectés de Windows 2000 peuvent voir une erreur semblable à ce en cas visualiseur, log système :

```
Event Type:     Error

Event Source:   Service Control Manager

Event Category: None

Event ID:       7031

Date:           8/11/2003

Time:           10:10:10 PM

User:           N/A
```

```
Computer:       COMPUTER

Description:

The Remote Procedure Call (RPC) service terminated unexpectedly.
```
Le logiciel affecté est :

- Windows Server 2000
- Toutes les versions de Cisco CallManager

Solutions

Les solutions au problème sont expliquées en détail ici.

Si votre ordinateur n'est pas infecté par le virus

Terminez-vous ces étapes pour empêcher le virus d'infecter votre ordinateur.

1. Si vous exécutez le Cisco CallManager avec PRE-WinOSUpgrade2000-2-4, alors améliorez au **Cisco CallManager WinOS2000-2-4** et appliquez **WinOS2000-2-4sr5**.Si vous exécutez une version de Cisco CallManager qui a déjà WinOS2000-2-4, alors mise à jour au **Cisco CallManager WinOSUpgrade2000-2-4sr5**. Supplémentaire, si vous exécutez WinOSUpgradev2000-2-3 ou 2000-2-4, vous pouvez appliquer le correctif simple **MS03-026** pour corriger cette une bogue.
2. Après que vous appliquiez le correctif, vérifiez cette clé de registre :
   ```
   HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

   "windows auto update"="msblast.exe"
   ```
   Si cette clé est présente, alors il est probable votre système est déjà infecté. Envisagez d'exécuter l'outil de virus de Stinger ou tout autre logiciel de virus répertorié dans si votre ordinateur est infecté par la section de virus.

Si votre ordinateur est infecté par le virus

Si votre ordinateur est déjà infecté, les mises à jour décrites plus tôt dans ce document ne retirent pas le virus. Exécutez ces étapes avant que vous appliquiez le correctif de Microsoft.

1. Basé sur votre logiciel de virus vous avez besoin de l'un ou l'autre obtenez le dernier fichier 4284 DAT de McAfee, qui a définitions de définitions de suppression de virus les dernières ou de virus de Norton, qui ont été récemment libérées.**Note**: Norton est seulement pris en charge pour l'application de Cisco CallManager.Si votre système est infecté et n'a pas Norton ou McAfee sur le système, vous pouvez envisager d'exécuter seul de support l'outil Stinger v1.8.0 de suppression de virus .
2. Améliorez le Cisco CallManager aux releases mentionnées dans si votre ordinateur n'est pas infecté par la section de virus. En outre, assurez-vous que tous les téléchargements (MS03-026) pour le Cisco CallManager soyez de cisco.com et pas du site de Microsoft.

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