AVVIDネットワークにおける Code Red II の緊急障害復旧の手順

目次

概要

このドキュメントでは、蔓延している Code Red II の感染のために生じる Cisco CallManager の症状のほとんどを緊急に排除する手順について説明します。同時に、将来において同様の問題から AVVID ネットワークを保護するための当面の解決策や長期にわたる解決策についても説明します。

前提条件

要件

このドキュメントの読者は次のトピックについて理解している必要があります。

- Cisco CallManager の管理
- 緊急的な障害回復手順

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco CallManager 3.x
- Microsoft Windows 2000
- Cisco Unity のすべてのバージョン

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

即時の処置

次の手順を実行します。

1. 最新の win-OS-upgrade（CCO にある CallManager のバージョン ダウンロード ページの暗号化セクションから入手可能）を、Windows 2000 が稼働しているすべての IP テレフォニー サーバ上で実行します。さらに、適切な修復ユーティリティ（Microsoft からツールが公開）の実行と、Code Red II によって作成されたバックドアの手作業での（McAfee で公開）閉鎖のいずれか、あるいは両方を実行します。 NT4.0 IIS が稼働している IP テレフォニー サーバ の場合は、Service Pack 6a をインストールして、次に Code Red fix を実行します。**注意：** 注意：このワームはバックドアを作成します。そのため、サーバがインターネットに直接接続されていて、侵入を受けている間に何者かによってさらに多数のバックドアが作成された可能性がある場合や、現在のネットワーク内からサーバがさらに侵入を受けている可能性がある場合には、データをバックアップして、サーバを最初から再インストールすることが最も安全な対策になります。
2. IIS Admin Service と World Wide Web Publishing サービスをすべての Cisco CallManager 登録者に対して停止およびディセーブルにします。また、このサービスが必要でない全サーバに対しても行います。 これらのサービスは、Cisco CallManager Publisher 上ではアクティブのままにしておく必要があります。この作業を実行するには、次の手順を従ってください。**[Start] > [Programs] > [Administrative Tools] > [Services]** に移動し、サービス ア>プレットを起動します。IIS Admin Service を右クリックして、Stop を選択します。 これによって、World Wide Web Publishing サービスも停止します。IIS Admin Service を右クリックして、Properties を選択します。 [Startup Type] を **[Disable]** に変更して、ウィンドウを閉じます。**[World Wide Web Publishing]** を右クリックして、**[Properties]** を選択します。 [Startup Type] を **[Disable]** に変更して、ウィンドウを閉じます。
3. ネットワーク上の既知のすべての IIS サーバにパッチを適用するか、修復します。
4. 更新された電話ロードを導入します。Cisco CallManager 3.0x システムの場合は、ciscocm_3-0-11_spA.exe を Cisco.com からダウンロードします。 [CCMAdmin] ページから **[System] > [Device Defaults]** に移動し、[7940/7960 Device Loads] >に **[P003E310]** を設定します。 [Update] をクリックします。Cisco CallManager 3.1x システムの場合は、ciscocm_3-1-1_spA.exe を Cisco.com からダウンロードします。 [CCMAdmin] ページから **[System] > [Device Defaults]** に移動し、[7940/7960 Device Loads] >に **[P00303010100]** を設定します。 [Update] をクリックします。Cisco CallManager 3.0 および 3.1 の場合、**[System] > [CallManager Group]** に移動します。 左側にある最初のグループを選択して、Reset Devices をクリックして、プロンプトが表示されたら OK を選択します。 この作業を電話で構成されている各 Cisco CallManager グループに対して繰り返し、新しいロードを入手できるようにします。Cisco CallManager 3.2x および 3.3x のシステムでは、必要な修復すべてが含まれているため、更新された電話ロードを必要としません。
5. ネットワーク上のその他の感染 IIS サーバを特定して対処します。ネットワーク上に被害を受けた IIS サーバがいくつあるかによって、当面の解決策に進みやすくなります。 次に 2 つの方法を示します。Cisco CallManager Publishing サーバか、ロギングが有効になっている他の IIS サーバで、**c:\winnt\system32\logfiles\w3svc1** に移動して最新のログ ファイルにアクセスします。 これらのファイルの命名規則は、ex000000.log となっています。次のよう

な行を探します。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 -この場合、IP アドレスは 172.20.148.189 は、攻撃しているサーバです。 これを探してパッチを適用するかワームを除去します。あるいは、ネットワークから切り離します。Code Red に感染したすべてのサーバが判明して対応が終わるまで、この操作を繰り返します。もう 1 つの方法は、eEye から入手可能な無料のユーティリティを使用することです。 - CodeRedScanner。 このユーティリティは、感染したマシンおよび .ida ベースの攻撃に対して脆弱なマシンを見つけるための 1 つのクラス C を同時にスキャンします。 eEye には、追加コストを払えば利用可能なクラス B のスキャナがあります。

短期的なソリューション

- 音声トラフィックがデータ トラフィックよりも優先されるよう、Quality of Service（QoS）がネットワーク全体で正しく設定されていることを確認します。 残りのクリーンアップ処理中の音声品質への影響を確実に最小化するには、『シスコのネットワーク ソリューションと QoS の設計ガイド』および『Cisco IP Telephony ソリューションの設計ガイド』に記述されている推奨事項を参照してください。
- 音声用とデータ用の VLAN を別々に構築するには、『Cisco IP Telephony ソリューション』のリソースに従ってください。 これは、対象とするネットワークの規模と複雑性によっては、長期にわたる解決策となる場合もあります。

長期的なソリューション

即時に対応が必要な緊急事態が去ったら、『安全： IP テレフォニー セキュリティの詳細』を参照してください。 このドキュメントには、安全な IP 電話ネットワークの設計と実装に関心のある読者向けに、ベストプラクティスとなる情報が記載されています。

関連情報

- 音声に関する技術サポート
- 音声とユニファイド コミュニケーションに関する製品サポート
- Cisco IP Telephony のトラブルシューティング
- テクニカルサポートとドキュメント - Cisco Systems