# AVVID 网络的红色代码 II 紧急灾难恢复过程

## 目录



## 简介

本文包括步骤立即排除大多副作用到Cisco CallManager由于一普遍红色代码II传染，与近和长期解决方案一起改善安全和在将来保护从相关问题的一个AVVID网络。

## 先决条件

### 要求

本文档的读者应掌握以下这些主题的相关知识：

- Cisco CallManager管理
- 紧急灾难恢复程序

### 使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco CallManager 3.x
- Microsoft Windows 2000
- Cisco Unity所有版本

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

### 规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

# 即时动作

完成这些步骤：

1. 运行最新的win OS升级(在适当的Callmanager版本下载页的crypto部分的联机在CCO的)在运行Windows 2000的所有IP电话服务器，并且运行适当的修理工具(Microsoft有工具联机)并且/或者(从McAfee的可得到)请手工关闭红色代码创建的后门II。对于运行NT4.0 IIS的IP电话服务器，请安装服务包6a然后红色代码修正。**警告：** 由于此蠕虫病毒创建后门，如果服务器直接地连接到互联网，并且某人在它可能安置了更多后门，当折衷了时，或者，如果进一步折衷从您的网络的内部服务器的可能性存在，最安全的操作是备份数据和从头重新安装服务器。
2. 中断并且禁用IIS Admin服务和Web发布服务在所有Cisco CallManager用户和不要求他们的所有服务器。这些服务一定依然是活动在Cisco CallManager发布器。要执行此任务，请遵从这些步骤：通过去启动服务applet **Start > Programs > Administrative Tools > Services**。用鼠标右键单击**IIS Admin服务**并且选择**终止**。这也终止Web发布服务。右键单击**IIS Admin服务**和选择**属性**。更改起始类型**禁用**，并且关上窗口。用鼠标右键单击**发布的全球资讯网**并且选择**属性**。更改起始类型**禁用**，并且关上窗口。
3. 修补或修复在网络的所有已知IIS服务器。
4. deploy更新电话负载。Cisco CallManager 3.0x系统，从Cisco.com的下载ciscocm_3-0-11_spA.exe。从Ccmadmin页请去**System > Device Defaults**并且设置7940/7960设备加载为**P003E310**。单击**更新**。对于Cisco CallManager 3.1x系统，请下载从Cisco.com的ciscocm_3-1-1_spA.exe。从Ccmadmin页请去**System > Device Defaults**并且设置7940/7960设备加载为**P00303010100**。单击**更新**。对于两Cisco CallManager 3.0和3.1，请去**系统> Callmanager组**。选择在左手边的第一组，并且点击**"Reset"设备**，挑选**OK，**当提示。为每Cisco CallManager组执行此当前为了电话能获得他们新的负载。因为他们包括所有必要的修正，Cisco CallManager 3.2x和3.3x系统不要求一更新电话负载。
5. 识别并且照料剩余在网络的被传染的IIS服务器(这可能容易地拉伸到近期解决方案，根据多少个恶意IIS服务器在网络)。这是两个方法：在Cisco CallManager发布服务器，或者其他IIS服务器上有启用的记录日志的，请去**c:\winnt\system32\logfiles\w3svc1**并且访问最最近的日志文件。这些文件有ex000000.log命名规则。寻找一条线路类似于此：

   ```
   2001-08-09 00:11:57 172.20.148.189 - 172.20.225.130 80 GET /default.ida
   XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
   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 -
   ```

   在这种情况下， IP地址172.20.148.189是攻击的服务器。查找它并且修补或者清洗它或者从网络断开它。请重复此进程，直到所有剩余的代码Red-infected服务器查找和已处理。另一个方法将使用从eEye的免费工具程序可得到 - CodeRedScanner。此工具每次扫描寻找受感染的机器和机器的一C类易受到.ida基于攻击。eEye有一个增加成本的B类扫描仪联机。

# 近期解决方案

- 保证您有服务质量(QoS)适当地配置在您的网络中指定优先级在数据流的语音流量。要帮助保证在清理操作期间，剩余语音质量尽可能少受影响，参考在思科网络解决方案提供的建议和QoS设计指南和Cisco IP电话解决方案设计指南。
- 设立分离的语音和数据VLAN，跟随Cisco IP电话解决方案资源。这能是长期解决方案根据介入的网络的大小和复杂性。

## 长期解决方案

一旦立即紧急情况结束，参考SAFE ：详细的IP电话安全。本文提供最佳方法信息给主要负责人为设计和实现安全IP电话网络。

## 相关信息

- 语音技术支持
- 语音和统一通信产品支持
- Cisco IP 电话故障排除
- 技术支持和文档 - Cisco Systems