

Code Red II Emergency Disaster Recovery Procedures for an AVVID Network

Document ID: 5200

Introduction

Prerequisites

Requirements

Components Used

Conventions

Immediate Actions

Near-Term Solutions

Long-Term Solutions

NetPro Discussion Forums – Featured Conversations

Related Information

Introduction

This document covers the procedures to immediately eliminate most of the side effects to Cisco CallManager due to a widespread Code Red II infection, along with near- and long-term solutions to better secure and protect an AVVID network from related problems in the future.

Prerequisites

Requirements

Readers of this document should have knowledge of these topics:

- Cisco CallManager administration
- Emergency disaster recovery procedure

Components Used

The information in this document is based on these software and hardware versions:

- Cisco CallManager 3.x
- Microsoft Windows 2000
- All versions of Cisco Unity

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Immediate Actions

Complete these steps:

1. Run the latest win-OS-upgrade (available in the crypto section of the appropriate CallManager version download page on CCO) on all IP Telephony Servers running Windows 2000, and run the appropriate repair utility (Microsoft has a tool available) and/or manually (available from McAfee) close the backdoors created by Code Red II. For IP Telephony Servers running NT4.0 IIS, install Service Pack 6a and then the Code Red fix.



Caution: Because this worm creates backdoors, if the server was directly connected to the

Internet and someone could have placed more backdoors in it while it was compromised, or if the possibility of the server being further compromised from within your network exists, the safest action would be to backup the data and reinstall the server from scratch.

2. Stop and disable IIS Admin Service and World Wide Web Publishing service on all Cisco CallManager subscribers, and any server that does not require them. These services must remain active on the Cisco CallManager Publisher.

To perform this task, follow these steps:

- a. Bring up the services applet by going to **Start > Programs > Administrative Tools > Services**.
 - b. Right-click **IIS Admin Service** and select **Stop**. This also stops the World Wide Web Publishing service.
 - c. Right-click **IIS Admin Service** and select **Properties**. Change Startup Type to **Disable**, and close the window.
 - d. Right-click **World Wide Web Publishing** and select **Properties**. Change Startup Type to **Disable**, and close the window.
3. Patch or repair all known IIS servers in the network.
 4. Deploy updated phone loads.
 - ◆ For Cisco CallManager 3.0x systems, download ciscocm_3-0-11_spA.exe from Cisco.com. From the CCMAAdmin page go to **System > Device Defaults** and set the 7940/7960 Device Loads to **P003E310**. Click **Update**.
 - ◆ For Cisco CallManager 3.1x systems, download ciscocm_3-1-1_spA.exe from Cisco.com. From the CCMAAdmin page go to **System > Device Defaults** and set the 7940/7960 Device Loads to **P00303010100**. Click **Update**.
 - ◆ For both Cisco CallManager 3.0 and 3.1, Go to **System > CallManager Group**. Select the first group on the left hand side, and click **Reset Devices**, select **OK** when prompted. Do this for each Cisco CallManager group present for the phones to get their new loads.
 - ◆ Cisco CallManager 3.2x and 3.3x systems do not require an updated phone load, as they include all necessary fixes.
 5. Identify and take care of remaining infected IIS servers on the network (this could easily stretch into a near-term solution, depending on how many rogue IIS servers are on the network). Here are two methods:

- ◆ On the Cisco CallManager Publishing server, or any other IIS server with logging enabled, go to **c:\winnt\system32\logfiles\w3svc1** and access the most recent log file. These files have a naming convention of ex000000.log.

Look for a line similar to this:

```

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
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 -

```

In this case, the IP address 172.20.148.189 is the attacking server. Find it and patch or clean it, or disconnect it from the network.

Repeat this process until all remaining Code Red–infected servers have been located and taken care of.

- ◆ Another method is to use the free utility available from eEye – CodeRedScanner . This utility scans one Class C at a time looking for infected machines and machines vulnerable to an .ida based attack. eEye has a Class B scanner available for an additional cost.

Near–Term Solutions

- Ensure that you have Quality of Service (QoS) configured properly throughout your network to prioritize voice traffic over data traffic. To help ensure that voice quality is affected as little as possible during the remainder of cleanup operations, refer to the recommendations provided in the Cisco Networking Solutions and QoS Design Guides and the Cisco IP Telephony Solution Design Guides.
- Establish separate voice and data VLANs, following the Cisco IP Telephony Solutions resources. This could be a long–term solution depending on the size and complexity of the network involved.

Long–Term Solutions

Once the immediate emergency is over, refer to SAFE: IP Telephony Security In Depth. This document provides best–practice information to interested parties for designing and implementing secure IP Telephony networks.

NetPro Discussion Forums – Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

NetPro Discussion Forums – Featured Conversations for Voice
Service Providers: Voice over IP
Voice & Video: Voice over IP
Voice & Video: IP Telephony
Voice & Video: IP Phone Services for End Users
Voice & Video: Unified Communications
Voice & Video: IP Phone Services for Developers
Voice & Video: General

Related Information

- [Voice Technology Support](#)
 - [Voice and IP Communications Product Support](#)
 - [Recommended Reading: Troubleshooting Cisco IP Telephony](#)
 - [Technical Support & Documentation – Cisco Systems](#)
-

All contents are Copyright © 2006–2007 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Updated: Feb 02, 2006

Document ID: 5200
