

Cleaning Nimda Virus from Cisco CallManager 3.x and CallManager Applications Servers

Document ID: 13971

Introduction

Prerequisites

Requirements

Components Used

Conventions

Clean Cisco CallManager/Applications Servers

NetPro Discussion Forums – Featured Conversations

Related Information

Introduction

This document explains the procedure you use in order to clean the Nimda virus from Cisco CallManager and Cisco CallManager application servers.

Prerequisites

Requirements

There are no specific requirements for this document.

Note: Always make sure that your Cisco CallManager Server has the necessary virus protection. Refer Using McAfee NetShield with Cisco CallManager for more information.

Components Used

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

- Cisco CallManager up to 3.3(3) (This is because Cisco CallManager 3.3(4) and later require OS2000.2.5sr2 prior to the upgrade/install. The fix is in OS2000.2.5.)

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

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Clean Cisco CallManager/Applications Servers

Complete these steps:

1. Perform an MCS Backup using the Cisco provided Cisco IP Telephony Application Backup Utility. If you already have a current backup, continue with the next step.

2. Ensure you do not have shared drives to any machines that are infected, as the worm can spread via shared drives.
3. Stop the **IIS Admin service** on the machine that is infected. (This also stops FTP and WWW services.)
4. Download and run the **win-OS-Upgrade.2000-2-5.exe** (registered customers only) and the latest service update for this upgrade available on Cisco.com. This requires at least one reboot.
5. As a precaution for possible Code Red II vulnerabilities, download the **Code Red II Cleanup** tool from Microsoft.

Due to product licensing issues Cisco cannot distribute this tool.

6. Several antivirus companies have produced tools to eliminate the Nimda virus. Cisco has tested the Nimda Cleanup tool from Network Associates and has confirmed that it cleans a Cisco CallManager server with no damaging side effects.

Due to product licensing issues Cisco cannot distribute this tool. Please contact Network Associates directly to obtain the latest version of this tool.

7. Navigate to the directory where you downloaded the CodeRedCleanup.exe file and run it.
8. Navigate to the directory where you downloaded the Nimda Cleanup tool and run it on the C: drive.
9. After step 8 is finished, run the Nimda Cleanup tool on the E: drive.
10. Cisco CallManagers should only have a C: and an E: hard drive partition. Drive D: is usually the CD-ROM drive. If the server has any other hard drives, run the Nimda Cleanup tool on those drives as well.

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 Unified Communications Product Support**
- **Recommended Reading: Troubleshooting Cisco IP Telephony**
- **Technical Support & Documentation – Cisco Systems**

