

Defend Against the Sasser Virus on the MCS Servers

Document ID: 51361

Introduction

Prerequisites

Requirements

Components Used

Conventions

Problem

Solutions

Protect Your Computer

Protect CallManager

Protect Unity

Related Information

Introduction

This Document is intended to assist Cisco Architecture for Voice, Video, and Integrated Data (Cisco AVVID) customers with means to resolve the effects of the W32/Sasser.worm.b virus. This self-executing worm spreads by exploiting a Microsoft Windows vulnerability (MS04-011 vulnerability [CAN-2003-0533]). The worm spreads with the file name avserve2.exe. Unlike many recent worms, this virus does not spread through email. No user intervention is required to become infected or propagate the virus further. The worm works by instructing vulnerable systems to download and execute the viral code.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

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

- All types of Cisco CallManager servers
- All types of Cisco Unity servers

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.

Problem

The virus copies itself to the Windows directory as avserve2.exe and creates a registry run key to load itself at startup:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\ CurrentVersion\Run "avserve2.exe" =  
C:\WINDOWS\avserve2.exe
```

As the worm scans random IP addresses it listens on successive TCP ports starting at 1068. It also acts as an FTP server on TCP port 5554, and creates a remote shell on TCP port 9996.

A file named win2.log is created on the root of the C: drive. This file contains an IP address.

Copies of the worm are created in the Windows System directory as #_up.exe:

- C:\WINDOWS\system32\11583_up.exe
- C:\WINDOWS\system32\16913_up.exe
- C:\WINDOWS\system32\29739_up.exe

A side-effect of the worm is for LSASS.EXE to crash, by default the system reboots after the crash occurs.

This worm scans random IP addresses for exploitable systems. When one is found, the worm exploits the vulnerable system by overflowing a buffer in LSASS.EXE. It creates a remote shell on TCP port 9996. Next, it creates an FTP script named cmd.ftp on the remote host and executes it. This FTP script instructs the target victim to download and execute the worm (with the filename #_up.exe as mentioned earlier) from the infected host. The infected host accepts this FTP traffic on TCP port 5554.

The worm spawns multiple threads, some of which scan the local class A subnet, others the class B subnet, and others completely random subnets. The destination port is TCP 445.

All types of Cisco CallManager and Unity servers are affected.

For more information how it spreads, refer to McAfee Security's Virus Profile .

Solutions

Use these solutions to solve the problem.

Protect Your Computer

For information on protecting your computer from the virus, refer to What You Should Know About the Sasser Worm and Its Variants . This page also includes a link to run a program to remove the virus after the patch has been installed.

Protect CallManager

To protect Cisco CallManager, refer to CallManager and Voice Apps Crypto Software Download (registered customers only) and download the MS04-011 patch, which is found in Operating System Upgrade Service Release 2000-2-5sr8.

Note: You have to install this upgrade release and not apply the patch from Microsoft.

Protect Unity

Since MS04–011 is not a service pack, you can install it to a Cisco Unity server without Business Unit (BU) approval. For more information, refer to Microsoft Security Bulletin MS04–011 .

Related Information

- **Voice Technology Support**
 - **Voice and Unified Communications Product Support**
 - **Recommended Reading: Troubleshooting Cisco IP Telephony**
 - **Technical Support – Cisco Systems**
-

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2009 – 2010 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Feb 03, 2006

Document ID: 51361
