

MS/Windows W32.Blaster.Worm Affects Cisco CallManager

Document ID: 44465

Introduction

Prerequisites

Requirements

Components Used

Conventions

Problem – DCOM RPC Vulnerability

Problem Symptoms

Solutions

If Your Machine is NOT Infected with the Virus

If Your Machine IS Infected with the Virus

Related Information

Introduction

Microsoft Corporation recently announced a security vulnerability in its Windows Operating System(s), which allows attacks by the W32.Blaster.Worm to the Cisco CallManager server and the Cisco Conference Connection (CCC), Cisco Emergency Responder (CER), Cisco IP Contact Center (IPCC) Express and PA applications. This security vulnerability is in a Windows Distributed Component Object Model (DCOM) Remote Procedure Call (RPC) interface.

This virus may also be known as:

- W32/Lovsan.worm (NAI)
- Win32.Poza (CA)
- WORM_MSBLAST.A (Trend)

Additional information can be found on the Microsoft Website at these locations:

- Microsoft Security Bulletin MS03-026
- Virus Alert About the W32.Blaster.Worm Worm
- What You Should Know About the Blaster Worm

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

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

- Windows 2000 Server
- All Cisco CallManager versions
- CCC, CER, IPCC Express, ISN, and PA

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 – DCOM RPC Vulnerability

A stack-based buffer overflow condition has been discovered in the Microsoft RPC interface for DCOM. This is a core function of the Windows kernel, and cannot be disabled. Since this is a kernel function (implemented via SVCHOST.EXE), successful attacks result in System privilege. Specially crafted messages sent to port 135 exploit the buffer overflow.

Problem Symptoms

Exploit code circulates in the wild executes shell code after the buffer overflow. This allows remote access to a command shell and complete, privileged remote control of the system. You might possibly see an error in the Event Viewer on an infected system.

All infected Windows 2000 machines can see an error similar to this in the Event Viewer, System Log:

```
Event Type:      Error
Event Source:    Service Control Manager
Event Category:  None
Event ID:        7031
Date:            8/11/2003
Time:            10:10:10 PM
User:            N/A
Computer:        COMPUTER
Description:

The Remote Procedure Call (RPC) service terminated unexpectedly.
```

The software affected is:

- Windows Server 2000
- All versions of Cisco CallManager

Solutions

The solutions to this problem are explained in detail here.

If Your Machine is NOT Infected with the Virus

Complete these steps to prevent the virus from infecting your machine.

1. If you run Cisco CallManager with PRE-WinOSUpgrade2000-2-4, then upgrade to **Cisco CallManager WinOS2000-2-4** and apply **WinOS2000-2-4sr5**.

If you run a Cisco CallManager version that already has WinOS2000-2-4, then upgrade to **Cisco CallManager WinOSUpgrade2000-2-4sr5**. Additionally, if you run WinOSUpgrade2000-2-3 or 2000-2-4, you can apply the single hotfix **MS03-026** to patch this one bug.

2. After you apply the patch, check for this registry key:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run  
  
"windows auto update"="msblast.exe"
```

If this key is present, then it is likely your system is already infected. Consider running the Stinger virus tool or other virus software listed in the If Your Machine IS Infected with the Virus section.

If Your Machine IS Infected with the Virus

If your machine is already infected, the upgrades described earlier in this document do not remove the virus. Perform these steps before you apply the Microsoft patch.

1. Based on your virus software you need to either get McAfee's latest DAT file 4284, which has the virus removal definitions or Norton's latest virus definitions, which were recently released.

Note: Norton is only supported for the Cisco CallManager application.

If your system is infected and does not have Norton or McAfee on the system, you can consider running the stand alone virus removal tool Stinger v1.8.0 .

2. Upgrade the Cisco CallManager to the releases mentioned in the If Your Machine is NOT Infected with the Virus section. Also, make sure all downloads (MS03-026) for Cisco CallManager are from cisco.com and not Microsoft's site.

Related Information

- [Voice Technology Support](#)
- [Voice and Unified Communications Product Support](#)
- [Recommended Reading: Troubleshooting Cisco IP Telephony](#)
- [Technical Support & Documentation – 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: 44465
