# CallManager da Cisco e aplicativos de telefonia IP das influências do W32.Blaster.Worm de MS Windows

## Índice



## Introdução

Microsoft Corporation anunciou recentemente uma vulnerabilidade de segurança em seu sistema operacional de Windows, que permite ataques pelo W32.Blaster.Worm ao servidor do CallManager da Cisco e ao Cisco Conference Connection (CCC), o Cisco Emergency Responder (CER), Cisco IP Contact Center (IPCC) expressa e aplicativos PA. Essa vulnerabilidade de segurança está em uma interface de Chamada de procedimento remoto (RPC) do Modelo de objeto de componentes distribuídos (DCOM) do Windows.

Este vírus pode igualmente ser sabido como:

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

A informação adicional pode ser encontrada na site do microsoft nestes lugar:

- Boletim de segurança MS03-026 de Microsoft
- Alerta do vírus sobre o worm do W32.Blaster.Worm
- O que você deve saber sobre o worm do dinamitador

## Pré-requisitos

### Requisitos

Não existem requisitos específicos para este documento.

## Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Windows Server 2000
- Todas as versões do CallManager da Cisco
- CCC, CER, IPCC expresso, ISN, e PA

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

## Convenções

Para obter mais informações sobre convenções de documento, consulte as Convenções de dicas técnicas Cisco.

# Problema - Vulnerabilidade de DCOM RPC

Uma condição de excesso de buffer com base em pilha foi descoberta na interface Microsoft RPC para DCOM. Essa é uma função central do kernel do Windows e não pode ser desativada. Desde que esta é uma função de núcleo (executada através do SVCHOST.EXE), os ataques bem-sucedidos conduzem ao privilégio do sistema. Mensagens especialmente preparadas enviadas à porta 135 exploram o excesso de buffer.

## Sintomas do problema

O código da façanha circula no selvagem executa o código do shell após o excesso de buffer. Isto permite o Acesso remoto a um comando shell e a um controle remoto completo, privilegiado do sistema. Você pôde possivelmente ver um erro no visualizador de eventos em um sistema infectado.

Todas as máquinas contaminadas do Windows 2000 podem ver um erro similar a este no visualizador de eventos, log de sistema:

```
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.
```
O software afetado é:

- Windows Server 2000
- Todas as versões do CallManager da Cisco

# Soluções

As soluções a este problema são explicadas em detalhe aqui.

## Se sua máquina não é contaminada com o vírus

Termine estas etapas para impedir que o vírus contamine sua máquina.

1. Se você executa o CallManager da Cisco com PRE-WinOSUpgrade2000-2-4, a seguir promova ao **CallManager da Cisco WinOS2000-2-4** e aplique **WinOS2000-2-4sr5**.Se você executa uma versão do CallManager da Cisco que já tenha WinOS2000-2-4, a seguir elevação ao **CallManager da Cisco WinOSUpgrade2000-2-4sr5**. Adicionalmente, se você executa WinOSUpgradev2000-2-3 ou 2000-2-4, você pode aplicar o único hotfix **MS03-026** para remendar este um erro.
2. Depois que você aplica a correção de programa, verifique para ver se há esta chave de registro:
   ```
   HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

   "windows auto update"="msblast.exe"
   ```
   Se esta chave esta presente, a seguir é provável seu sistema está contaminado já. Consider que executa a ferramenta do vírus do Stinger ou o outro software de vírus alistou no se sua máquina é contaminada com a seção de vírus.

## Se sua máquina é contaminada com o vírus

Se sua máquina é contaminada já, as elevações descritas mais cedo neste documento não removem o vírus. Execute estas etapas antes que você aplique o patch do microsoft.

1. Baseado em seu software de vírus você precisa o um ou outro obtém o arquivo o mais atrasado 4284 DAT da McAfee, que tem as definições de remoção de vírus ou as definições de vírus as mais atrasadas de Norton, que foram liberadas recentemente.**Note**: Norton é apoiado somente para o aplicativo do CallManager da Cisco.Se seu sistema é contaminado e não tem Norton ou a McAfee no sistema, você pode considerar executar do suporte o Stinger v1.8.0 da ferramenta da remoção de vírus apenas .
2. Promova o CallManager da Cisco às liberações mencionadas no se sua máquina não é contaminada com a seção de vírus. Também, certifique-se que todas as transferências (MS03-026) para o CallManager da Cisco seja de cisco.com e não do local de Microsoft.

# Informações Relacionadas

- Suporte à Tecnologia de Voz
- Suporte ao Produto de Voz e Comunicações Unificadas
- Troubleshooting da Telefonia IP Cisco
- Suporte Técnico e Documentação - Cisco Systems