微软视窗W32.Blaster.Worm影响Cisco CallManager和IP电话应用程序

目录

简介

微软公司最近发表了在其Windows操作系统的一个安全漏洞，由W32.Blaster.Worm对Cisco CallManager服务器和Cisco会议连接(CCC)， Cisco Emergency Responder (CER)， Cisco IP Contact Center (IPCC) Express和PA应用程序允许攻击。此安全漏洞在Windows分布式组件对象模型(DCOM) Remote Procedure Call (RPC)接口。

此病毒可能也叫作：

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

其他信息可以在这些位置的Microsoft网站找到：

- Microsoft安全公告MS03-026
- 关于W32.Blaster.Worm蠕虫病毒的病毒警报
- 什么您应该了解冲击波蠕虫

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Windows 2000服务器
- 所有Cisco CallManager版本
- CCC， CER， IPCC Express， ISN和PA

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

问题- DCOM RPC漏洞

一个基于堆积的缓冲区溢出情况在Microsoft RPC接口发现DCOM的。这是Windows内核的核心功能，并且不可能禁用。因为这是核函数(实现通过SVCHOST.EXE)，成功的攻击导致系统权限。对端口135检测安全漏洞代码的特别被制作的发送的消息缓冲区溢出。

问题症状

检测安全漏洞代码代码在通配执行shell代码流通在缓冲区溢出以后。这允许对系统的shell命令和完整，特许遥控的远程访问。您也许可能发现在事件查看器的一个错误在传染的系统。

所有被传染的Windows 2000机器能看到错误类似于此在事件查看器，系统日志：

```
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.
```

受影响的软件是：

- Windows服务器2000年
- Cisco CallManager所有版本

解决方案

对此问题的解决方案详细解释此处。

如果您的计算机没有感染病毒

完成这些步骤防止病毒传染您的计算机。

1. 如果运行Cisco CallManager以PRE-WinOSUpgrade2000-2-4，则请升级到**Cisco CallManager WinOS2000-2-4**并且应用**WinOS2000-2-4sr5**。如果运行已经有WinOS2000-2-4的Cisco CallManager版本，则对**Cisco CallManager WinOSUpgrade2000-2-4sr5的**升级。另外，如果运行WinOSUpgradev2000-2-3或2000-2-4，您能应用单个ICM Hotfixes **MS03-026**修补此一bug。
2. 在您应用补丁程序后，请检查此注册表项：
   ```
   HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

   "windows auto update"="msblast.exe"
   ```
   如果此密钥存在，则是可能的您的系统已经被传染。考虑运行在If Your Machine IS Infected with the Virus部分或其他病毒软件列出的有刺的动物病毒工具。

如果您的计算机感染病毒

如果您的计算机已经被传染，在本文描述的前升级不删除病毒。在您应用Microsoft补丁前，请执行这些步骤。

1. 基于您的病毒软件您需要任一获得McAfee的最新的DAT文件4284，有病毒删除定义或Norton's最新的病毒定义，最近发布。**注意：** Norton为Cisco CallManager应用程序只支持。如果您的系统被传染和没有Norton或McAfee在系统，您能考虑运行单独支架病毒删除工具有刺的动物v1.8.0 。
2. 升级Cisco CallManager到在If Your Machine is NOT Infected with the Virus部分提及的版本。并且，请确保所有下载(MS03-026) Cisco CallManager的是从cisco.com而不是Microsoft的站点。

相关信息

- **语音技术支持**
- **语音和统一通信产品支持**
- **Cisco IP 电话故障排除**
- **技术支持和文档 - Cisco Systems**