Cisco Security Advisory

Microsoft SQL Server 2000 Vulnerabilities in Cisco Products - MS02-061

Severity

Advisory ID: cisco-sa-20030126-ms02-061
Published: 2003 January 26 05:30 GMT
Version1.5: Final
Workarounds: See below

Download CVRF
Download PDF
Email

Cisco Security Vulnerability Policy

To learn about Cisco security vulnerability disclosure policies and publications, see the Security Vulnerability Policy. This document also contains instructions for obtaining fixed software and receiving security vulnerability information from Cisco.

Subscribe to Cisco Security Notifications

Subscribe

Summary

This advisory describes a vulnerability that affects Cisco products and applications incorporating the use of the Microsoft SQL Server 2000 or the Microsoft SQL Server 2000 Desktop Engine (MSDE 2000).

A number of vulnerabilities that have been discovered that enable an attacker to execute arbitrary code or perform a denial of service against the server. These vulnerabilities were discovered and publicly announced by Microsoft in their Microsoft Security Bulletins MS02-039, MS02-056, and MS02-061.

All Cisco products and applications that are using unpatched Microsoft SQL Server 2000 or MSDE 2000 are vulnerable.

This advisory is available at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20030126-ms02-061.

Affected Products

To determine if a product is vulnerable, review the list below. If the software versions or configuration information are provided, then only those combinations are vulnerable.

Vulnerable Products

- Cisco CallManager 3.3(x)
- Cisco Unity 3.x, 4.x
- Cisco Building Broadband Service Manager 5.1

Products Confirmed Not Vulnerable

No other Cisco product is currently known to be affected by this vulnerability.

Details

Implementations of the Microsoft SQL Server 2000 and MSDE 2000 are vulnerable to buffer overflows and denial of service attacks. These vulnerabilities can be exploited to execute arbitrary code on a computer system or to disrupt normal operation of the server.

The vulnerabilities have been described in more detail at:

http://www.microsoft.com/technet/security/virus/alerts/slammer.asp
http://www.microsoft.com/technet/security/bulletin/MS02-039.asp
http://www.microsoft.com/technet/security/bulletin/MS02-056.asp
http://www.microsoft.com/technet/security/bulletin/MS02-061.asp

Workarounds

Cisco has published a companion document at http://www.cisco.com/warp/public/707/cisco-sn-20030125-worm.shtml which provides network based workarounds to mitigate the effects of these vulnerabilities. Cisco also recommends applying the software based fixes to affected devices to completely resolve the vulnerability.

Fixed Software

Cisco CallManager

Customers running version 3.3(x) should install Cisco's cumulative SQL 2000 Hotfix, SQL2K-MS02-061.exe, from the following location:
http://www.cisco.com/tacpage/sw-center/telephony/crypto/voice-apps/.

Cisco Unity

Customers should follow the instructions found in http://www.cisco.com/warp/public/788/AVVID/unity3_4_slamworm.html for upgrading their Cisco Unity servers.

Cisco Building Broadband Service Manager

Software is now available on Cisco's website to patch BBSM 5.1. Version 5.0 and 5.2 are not vulnerable.

Before installing the security patch for this vulnerability, customers should install MSFIX1 and MSFIX2. Java Runtime 1.3.1 must also be installed after MSFIX1, but before MSFIX2.

Java Runtime 1.3.1_06 is available here:
http://java.sun.com/j2se/1.3/download.html

The patch is available at this location:
http://www.cisco.com/public/sw-center/sw-netmgmt.shtml

Instructions for installing service patches on BBSM can be found here:
http://www.cisco.com/univercd/cc/td/doc/product/aggr/bbsm/bbsm52/user/use52_05.htm#50416

Exploitation and Public Announcements

This issue is being exploited actively and has been discussed in numerous public announcements and messages.

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20030126-ms02-061

Revision History

Revision 1.0	26-Jan-2003	Initial Public Release
Revision 1.1	26-Jan-2003	Added new link (first link) under Details section.
Revision 1.2	26-Jan-2003	Added new information in Cisco Building Broadband Service Manager section.
Revision 1.3	27-Jan-2003	Added text to include MSDE 2000.
Revision 1.4	27-Jan-2003	Removed ICM and Cisco E-mail Manager from Affected Products as they are not vulnerable to this issue.
Revision 1.5	03-Feb-2003	Removed 5.0 from vulnerable versions of BBSM, updated Unity fixes with a more detailed link.
