

# Table of Contents

<b><u>Cisco Security Advisory: Cisco Security Advisory: Microsoft SQL Server 2000 Vulnerabilities in Cisco Products – MS02–061</u></b> .....	1
<u>Document ID: 40161</u> .....	1
<u>Revision 1.5 INTERIM</u> .....	1
<u>Last Updated 2003 February 03 18:00 GMT</u> .....	1
<u>For Public Release 2003 January 26 05:30 GMT</u> .....	1
<u>Please provide your feedback on this document</u> .....	1
<u>Summary</u> .....	1
<u>Affected Products</u> .....	1
<u>Details</u> .....	2
<u>Impact</u> .....	2
<u>Software Versions and Fixes</u> .....	2
<u>Obtain Fixed Software</u> .....	3
<u>Customers with Service Contracts</u> .....	3
<u>Customers using Third-party Support Organizations</u> .....	3
<u>Customers without Service Contracts</u> .....	3
<u>Workarounds</u> .....	4
<u>Exploitation and Public Announcements</u> .....	4
<u>Status of This Notice</u> .....	4
<u>Distribution</u> .....	4
<u>Revision History</u> .....	5
<u>Cisco Security Procedures</u> .....	5

# Cisco Security Advisory: Cisco Security Advisory: Microsoft SQL Server 2000 Vulnerabilities in Cisco Products – MS02–061

Document ID: 40161

## Revision 1.5 INTERIM

Last Updated 2003 February 03 18:00 GMT

For Public Release 2003 January 26 05:30 GMT

---

Please provide your feedback on this document.

---

**Summary**  
**Affected Products**  
**Details**  
**Impact**  
**Software Versions and Fixes**  
**Obtain Fixed Software**  
**Workarounds**  
**Exploitation and Public Announcements**  
**Distribution**  
**Revision History**  
**Cisco Security Procedures**

---

## Summary

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

A number of vulnerabilities that were discovered 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://www.cisco.com/warp/public/707/cisco-sa-20030126-ms02-061.shtml>.

## Affected Products

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

- Cisco CallManager 3.3(x)
- Cisco Unity 3.x, 4.x

- Cisco Building Broadband Service Manager 5.1

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

## Details

The 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>

## Impact

Microsoft says, the vulnerabilities range from an attacker gains additional privileges on a Structured Query Language (SQL) server in order to obtain control over the SQL Server. Additionally the MS SQL Sapphire Worm is known to exploit this same vulnerability which can result in degraded network performance as the worm attempts to propagate.

## Software Versions and Fixes

### Cisco CallManager

Customers who run version 3.3(x) must install the Cisco cumulative SQL 2000 Hotfix, SQL2K-MS02-061.exe, from this location:

<http://www.cisco.com/tacpage/sw-center/telephony/crypto/voice-apps/>.

### Cisco Unity

Customers must follow the instructions found in

[http://www.cisco.com/warp/public/788/AVVID/unity3\\_4\\_slamworm.html](http://www.cisco.com/warp/public/788/AVVID/unity3_4_slamworm.html) to upgrade their Cisco Unity servers.

### Cisco Building Broadband Service Manager

The software is now available on Cisco's website to patch Cisco Building Broadband Service Manager (BBSM) 5.1. Cisco Building Broadband Service Manager Version 5.0 and Building Broadband Service Manager 5.2 are not vulnerable.

Before you install the security patch for this vulnerability, you must 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 to install service patches on Cisco Building Broadband Service Manager can be found here:

[http://www.cisco.com/univercd/cc/td/doc/product/aggr/bbsm/bbsm52/user/use52\\_05.htm#50416](http://www.cisco.com/univercd/cc/td/doc/product/aggr/bbsm/bbsm52/user/use52_05.htm#50416)

When you consider software upgrades, refer to

[http://www.cisco.com/en/US/products/products\\_security\\_advisories\\_listing.html](http://www.cisco.com/en/US/products/products_security_advisories_listing.html) for consultation and any subsequent advisories to determine exposure and a complete upgrade solution.

In all cases, customers must exercise caution to be certain the devices to be upgraded contain sufficient memory and that current hardware and software configurations continue to be supported properly by the new release. If the information is not clear, contact the Cisco Technical Assistance Center (TAC) for assistance.

## Obtain Fixed Software

Where Cisco provides the operating system bundled with the product, Cisco offers free software upgrades to address these vulnerabilities for all affected customers. Customers can install and expect support for the feature sets they have purchased.

### Customers with Service Contracts

Customers with service contracts must contact their regular update channels to obtain any software release that contains the feature sets they have purchased. For most customers with service contracts, this means that upgrades must be obtained through the Software Center on Cisco's Worldwide Web site at <http://www.cisco.com/tacpage/sw-center/>.

### Customers using Third-party Support Organizations

Customers whose Cisco products are provided or maintained through a prior agreement or an agreement that exists with third-party support organizations such as Cisco Partners, authorized resellers, or service providers must contact that support organization for assistance to obtain the free software upgrade(s).

### Customers without Service Contracts

Customers who purchased directly from Cisco but who do not hold a Cisco service contract and customers who purchase through third-party vendors, are not able to obtain fixed software through their point of sale, must obtain fixed software through the Cisco Technical Assistance Center (TAC) with the help of the contact information listed here. In these cases, customers are permitted to obtain an upgrade to a later version of the same release or as indicated by the applicable row in the Software Versions and Fixes table.

Cisco TAC contacts are as follows:

- +1 800 553 2447 (toll free from within North America)
- +1 408 526 7209 (toll call from anywhere in the world)
- e-mail: [tac@cisco.com](mailto:tac@cisco.com)

For additional TAC contact information, which includes special localized telephone numbers and instructions and e-mail addresses for use in various languages, refer to

Cisco Security Advisory: Cisco Security Advisory: Microsoft SQL Server 2000 Vulnerabilities in Cisco Products

<http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>.

**Note:** You must have your product serial number available and give the URL of this notice as evidence of your entitlement to a free upgrade.

**Note:** *Do not* contact either "psirt@cisco.com" or "security-alert@cisco.com" for software upgrades.

Customers can only install and expect support for the feature sets they have purchased. By installation, download, access or otherwise with the help of such software upgrades, customers agree to be bound by the terms of Cisco's software license terms found at <http://www.cisco.com/public/sw-license-agreement.html>, or as otherwise set forth at Cisco.com Downloads at <http://www.cisco.com/public/sw-center/sw-usingswc.shtml>.

## 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 advises you to apply the software-based fixes to affected devices to completely resolve the vulnerability.

## Exploitation and Public Announcements

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

## Status of This Notice

This is a Interim advisory. Although Cisco cannot guarantee the accuracy of all statements in this notice, all of the facts have been checked to the best of Cisco's ability. Cisco does not anticipate to issue updated versions of this advisory unless there is some material change in the facts. If there is a significant change in the facts, Cisco is likely to update this advisory.

## Distribution

This notice is posted on Cisco's Worldwide Web site at <http://www.cisco.com/warp/public/707/cisco-sa-20030126-ms02-061.shtml>.

In addition to worldwide web posting, a text version of this notice is clear-signed with the Cisco PSIRT PGP key and is posted to these e-mail and Usenet news recipients:

- [cust-security-announce@cisco.com](mailto:cust-security-announce@cisco.com)
- [bugtraq@securityfocus.com](mailto:bugtraq@securityfocus.com)
- [full-disclosure@lists.netsys.com](mailto:full-disclosure@lists.netsys.com)
- [first-teams@first.org](mailto:first-teams@first.org) (includes CERT/CC)
- [cisco@spot.colorado.edu](mailto:cisco@spot.colorado.edu)
- [cisco-nsp@puck.nether.net](mailto:cisco-nsp@puck.nether.net)
- [comp.dcom.sys.cisco](mailto:comp.dcom.sys.cisco)
- [firewalls@lists.gnac.com](mailto:firewalls@lists.gnac.com)
- Various internal Cisco mailing lists

Future updates of this advisory, if any, will be placed on Cisco's Worldwide Web site, however they will not be actively announced on mailing lists or newsgroups. Users concerned about this problem are encouraged to check the above URL for any updates.

## 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 (BBSM) section.
Revision 1.3	27-Jan-2003	Added text to include MSDE 2000.
Revision 1.4	27-Jan-2003	Removed Cisco Intelligent Contact Management (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 Cisco Building Broadband Service Manager (BBSM), updated Unity fixes with a more detailed link.

## Cisco Security Procedures

For complete information on how to report security vulnerabilities in Cisco products, to obtain assistance with security incidents, and to register in order to receive security information from Cisco, visit [http://www.cisco.com/en/US/products/products\\_security\\_vulnerability\\_policy.html](http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html) on Cisco's Worldwide Web site.. This includes instructions for press inquiries with regard to Cisco security notices. All Cisco security advisories are available at <http://www.cisco.com/go/psirt>.

---

All contents are Copyright © 1992–2005 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

---

Updated: Jun 17, 2005

Document ID: 40161

---