



Release Notes for Cisco BBSM 5.1 Microsoft Buffer Overrun in RPCSS Service, Patch 5239

September 2003

These release notes describe the Cisco Building Broadband Service Manager (BBSM) 5.1 Microsoft buffer overrun in RPCSS Service vulnerability patch (RPCSSBufferOvrun.exe), which is also known as *Patch 5239*. This patch replaces patch 5231 and eliminates Microsoft security vulnerabilities on the BBSM 5.1 server. These vulnerabilities affect the Distributed Component Object Model (DCOM) interface, which handles DCOM object activation requests that are sent from one machine to another, within the RPCSS Service. This patch has no dependencies.



Note

The most current Cisco documentation for released products is available on Cisco Connection Online (CCO) at <http://www.cisco.com>. Online documents may contain updates and modifications made after the paper documents are printed.

Contents

- [Introduction, page 2](#)
- [Installation, page 2](#)
- [Obtaining Documentation, page 3](#)
- [Obtaining Technical Assistance, page 5](#)
- [Obtaining Additional Publications and Information, page 6](#)



Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Copyright © 2003 Cisco Systems, Inc. All rights reserved.

Introduction

Three new Microsoft vulnerabilities have been identified in the part of RPCSS Service that deals with Remote Procedure Call (RPC) messages for DCOM activation. These vulnerabilities result from incorrect handling of malformed messages and could allow arbitrary code execution and denial of service.

An attacker could exploit these vulnerabilities by creating a program that sends a malformed RPC message that targets the RPCSS Service on a vulnerable system. If successful, the attacker could run code with Local System privileges on the affected system or cause the RPCSS Service to fail. This would enable the attacker to remotely compromise a computer running Microsoft Windows and gain complete control over it.

For additional information, refer to this Microsoft website:

<http://www.microsoft.com/technet/security/bulletin/MS03-039.asp>

Installation

BBSM service packs and patches can be installed locally onto any BBSM server with Internet access, or they can be installed onto multiple BBSM servers from another computer in a remote location.

Follow these steps to install this patch onto your BBSM 5.1 server:

-
- Step 1** Using the Internet Explorer (IE) web browser, go to the Cisco BBSM 5.1 Software Download website:
<http://www.cisco.com/pcgi-bin/tablebuild.pl/bbsm51>



Note You must use the IE browser when using WEBpatch because of some known issues and incompatibilities with Netscape Navigator.

- Step 2** Download **RPCSSBufferOverrun.exe** to a temporary location on your computer.
- For a local BBSM installation, go to [Step 6](#).
 - For a remote BBSM installation, continue with [Step 3](#).



Note If you are using the Windows 2000 (SP2 or later) or Windows XP operating systems to install this patch remotely, the WEBpatch web pages load very slowly. To prevent this problem, uncheck the **Client for Microsoft Networks** check box in the NIC Properties window on your remote computer.

- Step 3** In the IE browser field, enter **http://<address>:9488/www** where <address> is either the external NIC address of the BBSM server (if you are accessing it externally) or the internal IP address of the BBSM server (if you are accessing it from within the BBSM subnet).

For example, enter **http://10.10.1.2:9488/www** and press **Enter**. The Enter Network Password window appears. (See [Figure 1](#).)

Figure 1 Enter Network Password Window



Step 4 Enter your username and password. (Do not enter any information in the Domain field.)



Note You must have administrator privileges to use WEBpatch.

Step 5 Click **OK**. The remote BBSM Dashboard appears.

Step 6 From the BBSM Dashboard, use the WEBpatch utility to install this patch.



Note Refer to the *Cisco BBSM 5.1 Software Configuration Guide* for instructions on transferring and installing BBSM patches and service packs. This patch automatically reboots your BBSM server.

Patch 5239 does not generate the *Reboot successful* patch log entry. You can verify that the MS03-039 patch is correctly installed by confirming that the following registry key exists: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Updates\Windows 2000\SP5\KB824146. For additional information, refer to Microsoft Knowledge Base Article - KB824146 at this website: <http://support.microsoft.com/?kbid=824146>.

Obtaining Documentation

Cisco provides several ways to obtain documentation, technical assistance, and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Related Documentation

The following documents provide information about BBSM:

- *Cisco BBSM 5.1 and BBSM Installation Guide* (order number DOC-7812741=)
- *Cisco BBSM 5.1 Software Configuration Guide* (available on Cisco.com)
- *Release Notes for the Cisco BBSM 5.1* (available on Cisco.com)

Cisco.com

You can access the most current Cisco documentation on the World Wide Web at this URL:

<http://www.cisco.com/univercd/home/home.htm>

You can access the Cisco website at this URL:

<http://www.cisco.com>

International Cisco websites can be accessed from this URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which may have shipped with your product. The Documentation CD-ROM is updated regularly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual or quarterly subscription.

Registered Cisco.com users can order a single Documentation CD-ROM (product number DOC-CONDOCCD=) through the Cisco Ordering tool:

http://www.cisco.com/en/US/partner/ordering/ordering_place_order_ordering_tool_launch.html

All users can order annual or quarterly subscriptions through the online Subscription Store:

<http://www.cisco.com/go/subscription>

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpk/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:
<http://www.cisco.com/en/US/partner/ordering/index.shtml>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit comments electronically on Cisco.com. On the Cisco Documentation home page, click **Feedback** at the top of the page.

You can send your comments in e-mail to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, the Cisco Technical Assistance Center (TAC) provides 24-hour, award-winning technical support services, online and over the phone. Cisco.com features the Cisco TAC website as an online starting point for technical assistance.

Cisco TAC Website

The Cisco TAC website (<http://www.cisco.com/tac>) provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The Cisco TAC website is available 24 hours a day, 365 days a year.

Accessing all the tools on the Cisco TAC website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a login ID or password, register at this URL:

<http://tools.cisco.com/RPF/register/register.do>

Opening a TAC Case

The online TAC Case Open Tool (<http://www.cisco.com/tac/caseopen>) is the fastest way to open P3 and P4 cases. (Your network is minimally impaired or you require product information). After you describe your situation, the TAC Case Open Tool automatically recommends resources for an immediate solution. If your issue is not resolved using these recommendations, your case will be assigned to a Cisco TAC engineer.

For P1 or P2 cases (your production network is down or severely degraded) or if you do not have Internet access, contact Cisco TAC by telephone. Cisco TAC engineers are assigned immediately to P1 and P2 cases to help keep your business operations running smoothly.

To open a case by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

For a complete listing of Cisco TAC contacts, go to this URL:

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

TAC Case Priority Definitions

To ensure that all cases are reported in a standard format, Cisco has established case priority definitions.

Priority 1 (P1)—Your network is “down” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Priority 2 (P2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

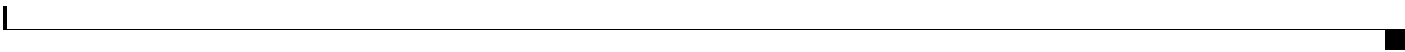
Priority 3 (P3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Priority 4 (P4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The *Cisco Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the *Cisco Product Catalog* at this URL:
http://www.cisco.com/en/US/products/products_catalog_links_launch.html
- Cisco Press publishes a wide range of networking publications. Cisco suggests these titles for new and experienced users: *Internetworking Terms and Acronyms Dictionary*, *Internetworking Technology Handbook*, *Internetworking Troubleshooting Guide*, and the *Internetworking Design Guide*. For current Cisco Press titles and other information, go to Cisco Press online at this URL:
<http://www.ciscopress.com>
- Packet magazine is the Cisco quarterly publication that provides the latest networking trends, technology breakthroughs, and Cisco products and solutions to help industry professionals get the most from their networking investment. Included are networking deployment and troubleshooting tips, configuration examples, customer case studies, tutorials and training, certification information, and links to numerous in-depth online resources. You can access Packet magazine at this URL:
<http://www.cisco.com/go/packet>
- iQ Magazine is the Cisco bimonthly publication that delivers the latest information about Internet business strategies for executives. You can access iQ Magazine at this URL:
<http://www.cisco.com/go/iqmagazine>
- Internet Protocol Journal is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:
http://www.cisco.com/en/US/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html
- Training—Cisco offers world-class networking training. Current offerings in network training are listed at this URL:
<http://www.cisco.com/en/US/learning/index.html>




This document is to be used in conjunction with the documents listed in the [Related Documentation](#) section.

CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, *Packet*, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0705R)

Copyright © 2003 Cisco Systems, Inc. All rights reserved.

 Printed in the USA on recycled paper containing 10% postconsumer waste.