



# Release Notes for Cisco BBSM 5.2 Web Proxy Vulnerability Fix, Patch 5246

---

## August 2004

These release notes describe the Cisco Building Broadband Service Manager (BBSM) 5.2 web proxy vulnerability patch and its installation. This patch (BBSM52Patch5246.exe) resolves a problem that enabled outside users to proxy through a BBSM server. Patch 5246 depends on BBSM 5.2 Service Pack 2 (SP2).

Cisco strongly recommends that you install this patch on all BBSM 5.2 SP2 servers.



### 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 4](#)
- [Documentation Feedback, page 5](#)
- [Obtaining Technical Assistance, page 5](#)
- [Obtaining Additional Publications and Information, page 7](#)



---

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

Copyright © 2004 Cisco Systems, Inc. All rights reserved.

# Introduction

This patch fixes a web proxy vulnerability that affects the BBSM 5.2 server. Vulnerable web proxy servers can be located by using available software tools. If the BBSM internal NIC is configured with a public IP address and this IP address becomes known, attackers could exploit this vulnerability to proxy traffic through the BBSM server.

We recommend that you install this patch for either of these conditions:

- If the internal NIC on your BBSM 5.2 server is configured with a public IP address
- If one-to-one static network address translation (NAT) is configured on the router or firewall to allow for remote management

After installing this patch, outside users will not be able to proxy through the BBSM 5.2 server.

# Installation

This section describes how to install the patch by using the Webpatch utility on BBSM. Read the Before You Start section before you begin the procedure.

You can install BBSM service packs or patches locally on any BBSM server or on multiple BBSM servers from another computer in a remote location. You can transfer multiple files to the BBSM server before you install them.

# Before You Start

Before you begin transferring and installing the patch, read the following:

- You must have administrator privileges to use WEBpatch.
- Make sure that both the external and internal NICs are plugged in and enabled, or the install will fail.
- Cisco strongly recommends that you terminate all client sessions during the installation and perform the installation during low-use time periods to minimize service interruptions and ensure proper functionality.
- Use Internet Explorer. Because of known issues with Netscape Navigator, you must use Internet Explorer when using the WEBpatch utility.
- If you are using Windows 2000 Professional or XP Professional on your client, uncheck the **Client for Microsoft Networks** check box as described below. When you uncheck this check box, the ASP files load much more quickly. Be sure to re-check it after you install the patch.
  - Choose **Start > Settings > Network and Dial-up Connections**. The Network and Dial-up Connections window appears.
  - Right-click **Local Area Connection**, and from the drop-down menu, choose **Properties**. The Local Area Connection Properties window appears.
  - Uncheck the **Client for Microsoft Networks** check box.
  - To close the windows, click **OK** three times.
- You must use the Java 2 plug-in, version 1.3.1\_03, to transfer patches. Other versions will fail. The Java plug-in must be installed on the remote computer that you are using to transfer the file. If the plug-in is not installed already, click **Go To Java Download Page**, download the plug-in, and install it.

- For additional information transferring and installing BBSM patches and service packs, refer to the *Cisco BBSM 5.2 User Guide*.

## Installing the Patch

Follow these steps to install this patch onto the BBSM 5.2 server:

- 
- Step 1** Using Internet Explorer, download **BBSM52Patch5246.exe** from the Cisco BBSM 5.2 Software Download website and save it in a temporary location on your computer:
- <http://www.cisco.com/cgi-bin/tablebuild.pl/bbsm52>
- To access the BBSM Dashboard remotely, continue with [Step 2](#).
  - To access the BBSM Dashboard from your local computer, go to [Step 3](#).
- Step 2** Launch Internet Explorer to access the BBSM server remotely on port 9488 instead of through the default web server port 80.
- Enter one of these URLs in the Internet Explorer address line:
    - To access BBSM from a remote location when you are not using SSL, enter this URL: **http://<external\_NIC\_address>:9488/www**, where <external\_NIC\_address> is the external network interface card (NIC) address of the BBSM server you want to access; for example, enter **http://10.10.1.2:9488/www** and press **Enter**. The Enter Network Password dialog box appears.
    - To access the BBSM Dashboard remotely through SSL, enter this URL: **https://<extNIC>/www** and press **Enter**. (You must have an SSL certificate installed on the BBSM server. The Enter Network Password dialog box appears.)
  - Enter your username and password and click **OK**. (Leave the Domain field blank.) The BBSM Dashboard appears.
- Step 3** From the BBSM Dashboard, use the WEBpatch utility to install the patch.
- From the BBSM Hotspot Dashboard, click **WEBpatch**. The BBSM Patches web page appears.
  - From the Installed patches drop-down menu, choose **BBSM52Patch5246.exe** and click **Go**. The BBSM Patches web page fields populate with the data for the patch, and the View Log Entries button is enabled.
  - Click **Transfer**. The BBSM Transfer web page appears.



**Caution** You must use the Java 2 plug-in, version 1.3.1\_03, to transfer patches. Other versions will fail. The Java plug-in must be installed on the remote computer that you are using to transfer the file. If the plug-in is not installed already, click **Go To Java Download Page**, download the plug-in, and install it.

- In the BBSM Transfer field, click **Browse** to navigate to the **BBSM52Patch5246.exe** file being installed and then click **Open**. The file name now appears in the BBSM Transfer field.
- Click **Transfer**. The BBSM WEBpatch Transferred web page appears, prompting you to install the file. (To install another file at the same time, click **Transfer** again to continue transferring files to be installed. After all files are transferred, continue with the installation.)
- Click **Go to Install** or **Install Patch**. The BBSM Install Patch web page appears:
  - If you clicked Go to Install, the page displays the transferred patch in the Select Self-Extracting Patch File to Install drop-down menu.

- If you clicked Install Patch, choose the patch from the Select Self-Extracting Patch File to Install drop-down menu.



**Note** This step may take a few minutes, depending on the size of the patch and whether you are remote or local.

- g. Click **Install**. The file is automatically verified and installed.



**Note** After the file has been installed, the BBSM server will automatically reboot. You cannot access the BBSM server while the server is rebooting.

**Step 4** To view the patch log to confirm that your patch installed successfully and to view any messages, follow these steps:

- a. Click **Patch Log**. The BBSM Patch Log web page appears. (This page can also be accessed from the Patches page by clicking **View Log Entries**.)
- b. From the drop-down menus at the top of the page, choose your criteria or click **Default**, which chooses all service packs and patches, the Summary trace level, and All log types.
- c. Click **Go**. The messages are displayed in the Patch Log Data table.
- d. Click **OK** to return to the Patch Log page and change the search parameters.

## Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

## Related Documentation

Refer to the following website for BBSM documentation and other release notes for BBSM 5.2:

[http://www.cisco.com/en/US/products/sw/netmgmtsw/ps533/prod\\_technical\\_documentation.html](http://www.cisco.com/en/US/products/sw/netmgmtsw/ps533/prod_technical_documentation.html)

Refer also to these specific BBSM documents:

- *Cisco BBSM 5.2 User Guide* (order number DOC-7814689=)
- *Cisco BBSM 5.2 and BBSD Software Installation Guide* (order number DOC-7812741=)
- *Cisco BBSM 5.2 Quick Start Guide* (order number DOC-7814813=)

## Cisco.com

You can access the most current Cisco documentation at this URL:

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

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

[http://www.cisco.com/public/countries\\_languages.shtml](http://www.cisco.com/public/countries_languages.shtml)

## Ordering Documentation

You can find instructions for ordering documentation at this URL:

[http://www.cisco.com/univercd/cc/td/doc/es\\_inpck/pdi.htm](http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm)

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:  
<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 send comments about technical documentation to [bug-doc@cisco.com](mailto: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, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

## Cisco Technical Support Website

The Cisco Technical Support Website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, 365 days a year at this URL:

<http://www.cisco.com/techsupport>

Access to all tools on the Cisco Technical Support Website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

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

## Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool automatically provides recommended solutions. If your issue is not resolved using the recommended resources, your service request will be assigned to a Cisco TAC engineer. The TAC Service Request Tool is located at this URL:

<http://www.cisco.com/techsupport/servicerequest>

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco TAC engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request 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 list of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/techsupport/contacts>

## Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

**Severity 1 (S1)**—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.

**Severity 2 (S2)**—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.

**Severity 3 (S3)**—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.

**Severity 4 (S4)**—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.

- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:  
<http://www.cisco.com/go/marketplace/>
- 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://cisco.com/univercd/cc/td/doc/pcat/>
- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:  
<http://www.ciscopress.com>
- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:  
<http://www.cisco.com/packet>
- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. 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/ipj>
- World-class networking training is available from Cisco. You can view current offerings 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.

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 © 2004 Cisco Systems, Inc. All rights reserved.

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