



# Release Notes for BBSM Hotspot 1.0 Microsoft Security Vulnerabilities Fix, Patch 5316

---

**May 2004**

These release notes describe the Cisco Building Broadband Service Manager (BBSM) Hotspot 1.0 Microsoft security vulnerabilities patch and its installation. This patch (Patch5316.exe) eliminates three Microsoft security vulnerabilities (MS04-011, MS04-012, and MS04-014) that affect the BBSM Hotspot server. Patch 5316 is dependent on BBSM Hotspot 1.0 Service Pack 1 (SP1).



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



---

**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 eliminates three Microsoft security vulnerabilities that affect the BBSM Hotspot 1.0 server. Attackers could exploit these vulnerabilities and gain complete control of an affected system. Attackers could then install programs, view, change, or delete data, or create new accounts with full system privileges. We recommend that you install this patch immediately.

- Security Update for Microsoft Windows (835732)

This update resolves newly-discovered vulnerabilities in Microsoft Windows. For additional information, refer to this Microsoft website:

<http://www.microsoft.com/technet/security/bulletin/MS04-011.msp>

- Cumulative Update for Microsoft RPC/DCOM (828741)

This update resolves newly-discovered vulnerabilities in Remote Procedure Call (RPC) and Distributed Component Object Model (DCOM). For additional information, refer to this Microsoft website:

<http://www.microsoft.com/technet/security/bulletin/MS04-012.msp>

- Vulnerability in the Microsoft Jet Database Engine Could Allow Code Execution (837001)

A buffer overrun vulnerability exists in the Microsoft Jet Database Engine that could allow remote code execution. For additional information, refer to this Microsoft website:

<http://www.microsoft.com/technet/security/bulletin/MS04-014.msp>

## Installation

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



### Caution

We recommend terminating all client sessions during BBSM service pack and patch upgrades and installations. For additional information, refer to the *Cisco BBSM Hotspot 1.0 User Guide*.

Follow these steps to install this patch onto the BBSM Hotspot 1.0 SP1 server:

- Step 1** Using the Internet Explorer (IE) web browser, go to the Cisco BBSM Hotspot 1.0 Software Download website:

<http://www.cisco.com/cgi-bin/tablebuild.pl/bbsm52>



### Note

Because of some known issues and incompatibilities with Netscape Navigator, you must use the IE browser when using WEBpatch.

- Step 2** Download **Patch5316.exe** to a temporary location on your computer.

- For a local BBSM installation, go to [Step 7](#).
- 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 remotely from within the BBSM subnet).

**Step 4** Press **Enter**. The Enter Network Password window appears.

**Step 5** Enter your username and password. (Do not enter any information in the Domain field.)

**Note**

You must have administrator privileges to use WEBpatch.

**Step 6** Click **OK**. The remote BBSM Dashboard appears.

**Step 7** From the BBSM Dashboard, click WEBpatch.

**Step 8** Verify that Service Pack 1 (Patch 5238) has been installed.

**Note**

Refer to the *Cisco BBSM Hotspot 1.0 User Guide* for instructions on verifying, transferring, and installing BBSM patches and service packs. This patch automatically reboots the BBSM Hotspot server after installation.

**Step 9** Install the patch using the WEBpatch utility.

## 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.

### 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\\_inpk/pdi.htm](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 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>

---

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 © 2004 Cisco Systems, Inc. All rights reserved.