



Release Notes for Cisco BBSM 5.1 ASN.1 Security Fix, Patch 5308

February 2004

These release notes describe the Microsoft Abstract Syntax Notation 1 (ASN.1) security vulnerability patch (MS04-007) and its installation. This patch (MS04-007SecurityPatch-5.1.exe) is also known as Patch 5308. This patch eliminates a buffer overrun security vulnerability on the Cisco Building Broadband Service Manager (BBSM) 5.1 server. Patch 5308 is dependent on BBSM MSFix1 (Patch 1061).



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 6](#)



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

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

Introduction

A Microsoft security vulnerability exists because of an unchecked buffer in the Microsoft ASN.1 Library. Attackers could exploit this vulnerability and cause a buffer overrun to occur, allowing them to gain control and execute code with system privileges on an affected system. This patch prevents an attacker from exploiting this vulnerability.

For additional information, refer to this Microsoft website:

<http://www.microsoft.com/technet/treeview/?url=/technet/security/bulletin/MS04-007.asp>

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 5.1 Software Configuration Guide*.

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/cgi-bin/tablebuild.pl/bbsm51>



Note

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

Step 2

Download **MS04-007SecurityPatch-5.1.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](#).



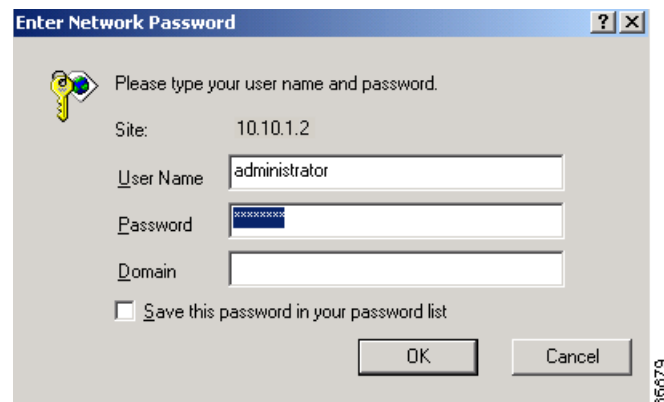
Note

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 the BBSM server.

Do not refer to the patch logs to verify that Patch 5308 installed correctly. The patch logs for Patch 5308 do not show the *InstallPatch completed* and *Reboot successful* logs. To verify that Patch 5308 (MS04-007) is installed, verify that the c:\WINNT\system32\msasn1.dll file is dated *19-Sep-2003* and its version number is *5.0.2195.6823*.

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

The following documents provide information about BBSM:

- *Cisco BBSM 5.1 and BBSD 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

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 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 submit e-mail comments about technical documentation 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-a-day, 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. If you do not hold a valid Cisco service contract, please contact your reseller.

Cisco TAC Website

The Cisco TAC website 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. The Cisco TAC website is located at this URL:

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

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

Using the online TAC Case Open Tool is the fastest way to open P3 and P4 cases. (P3 and P4 cases are those in which your network is minimally impaired or for which 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 the recommended resources, your case will be assigned to a Cisco TAC engineer. The online TAC Case Open Tool is located at this URL:

<http://www.cisco.com/tac/caseopen>

For P1 or P2 cases (P1 and P2 cases are those in which 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.

- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Go to this URL to visit the company store:
<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 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/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/ipj>
- 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 © 2004 Cisco Systems, Inc. All rights reserved.

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