

Cisco Security Advisory: Microsoft Windows SMB Denial of Service Vulnerabilities in Cisco Products – MS02–045

Document ID: 27111

Advisory ID: cisco-sa-20020918-smb-dos

<http://www.cisco.com/warp/public/707/cisco-sa-20020918-smb-dos.shtml>

Revision 1.1

Last Updated 2002 September 20 1800 UTC (GMT)

For Public Release 2002 September 18 1600 UTC (GMT)

Please provide your feedback on this document.

- Summary
- Affected Products
- Details
- Impact
- Software Versions and Fixes
- Workarounds
- Obtaining Fixed Software
- Exploitation and Public Announcements
- Status of This Notice: FINAL
- Distribution
- Revision History
- Cisco Security Procedures

Summary

This advisory describes vulnerabilities that affect Cisco products and applications that are installed on Microsoft operating systems incorporating the use of the Server Message Block (SMB) file sharing protocol. It is based on the vulnerabilities in Microsoft's SMB protocol, not due to a defect of the Cisco product or application.

Vulnerabilities were discovered that enable an attacker to perform a denial of service against the server and may allow execution of arbitrary code. These vulnerabilities were publicly announced by Microsoft in their Microsoft Security Bulletin MS02–045 .

All Cisco products and applications that are using the Microsoft operating systems identified by Microsoft in their Microsoft Security Bulletin MS02–045 are considered vulnerable.

This advisory is available at <http://www.cisco.com/warp/public/707/cisco-sa-20020918-smb-dos.shtml>.

Affected Products

This section provides details on affected products.

Vulnerable Products

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

- Cisco CallManager
- Cisco ICS 7750

Other products in the list below may be installed on the affected Microsoft operating systems and should have the hotfix from Microsoft installed to remove the vulnerabilities. This list is not all inclusive, please refer to Microsoft's bulletin if you think you have an affected Microsoft platform.

- Cisco Unity
- Cisco Building Broadband Service Manager (BBSM)
- Cisco uOne Enterprise Edition
- Cisco Network Registrar (CNR)
- Cisco Intelligent Contact Manager (ICM)
- Cisco E-mail Manager (CEM)
- Cisco Collaboration Server (CCS)
- Cisco Dynamic Content Adapter (DCA)
- Cisco Media Blender (CMB)
- TrailHead (Part of the Web Gateway solution)
- Cisco Works 2000
 - ◆ Lan Management Solution
 - ◆ Routed WAN Management
 - ◆ Service Management
 - ◆ VPN/Security Mangement Solution
 - ◆ IP Telephony Environment Monitor
 - ◆ Wireless Lan Solution Engine
 - ◆ Small Network Management Solution
 - ◆ QoS Policy Manager
 - ◆ Voice Manager
- Cisco Transport Manager (CTM)
- Cisco Broadband Troubleshooter (CBT)
- DOCSIS CPE Configurator
- Cisco Secure Applications
 - ◆ Cisco Secure Policy Manager (CSPM)
 - ◆ Access Control Server (ACS)

Products Confirmed Not Vulnerable

No other Cisco products are currently known to be affected by these vulnerabilities.

Details

The vulnerabilities have been described in more detail at <http://www.microsoft.com/technet/security/bulletin/MS02-045.asp> .

Impact

Successful exploitation of these vulnerabilities may cause the system to crash resulting in a loss of availability until the device has reinitialized.

Software Versions and Fixes

To access the software center for software fixes, you must be a registered user and you must be logged in.

Cisco CallManager

Version Affected	Fixed Regular Release (available now) Fix carries
Version 3.0.x	forward into all later versions Install win-OS-Upgrade.2000-1-3spF.exe from our Software Center
Version 3.1.x	Install win-OS-Upgrade.2000-1-3spF.exe from our Software Center
Version 3.2.x	Install win-OS-Upgrade.2000-1-3spF.exe from our Software Center

Cisco ICS 7750

Version Affected	Fixed Regular Release (available now) Fix carries
Version 1.x	forward into all later versions Follow instructions in the Field Notice Upgrade Program for SPE200 Then install win-OS-Upgrade.2000-1-3spF.exe from our Software Center
Version 2.x	Install win-OS-Upgrade.2000-1-3spF.exe from our Software Center

All Other Products

Install the patch for MS02-045 .

Workarounds

Microsoft documents several workarounds in their bulletin MS02-045 .

Obtaining Fixed Software

Cisco has made free software available to address this vulnerability for affected customers. Prior to deploying software, customers should consult their maintenance provider or check the software for feature set compatibility and known issues specific to their environment.

Customers may only install and expect support for the feature sets they have purchased. By installing, downloading, accessing or otherwise using 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>.

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

Customers with Service Contracts

Customers with contracts should obtain upgraded software through their regular update channels. For most customers, this means that upgrades should be obtained through the Software Center on Cisco's worldwide website at <http://www.cisco.com>.

Customers using Third-party Support Organizations

Customers whose Cisco products are provided or maintained through prior or existing agreement with third-party support organizations such as Cisco Partners, authorized resellers, or service providers should contact that support organization for guidance and assistance with the appropriate course of action in regards to this advisory.

The effectiveness of any workaround or fix is dependent on specific customer situations such as product mix, network topology, traffic behavior, and organizational mission. Due to the variety of affected products and releases, customers should consult with their service provider or support organization to ensure any applied workaround or fix is the most appropriate for use in the intended network before it is deployed.

Customers without Service Contracts

Customers who purchase direct from Cisco but who do not hold a Cisco service contract and customers who purchase through third-party vendors but are unsuccessful at obtaining fixed software through their point of sale should get their upgrades by contacting the Cisco Technical Assistance Center (TAC). 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

Have your product serial number available and give the URL of this notice as evidence of your entitlement to a free upgrade. Free upgrades for non-contract customers must be requested through the TAC.

Refer to <http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml> for additional TAC contact information, including special localized telephone numbers and instructions and e-mail addresses for use in various languages.

Exploitation and Public Announcements

The vulnerabilities described here have been discussed publicly on mailing lists and via security advisories released by other sources. Exploit code for these vulnerabilities is publicly available via the Internet.

Status of This Notice: FINAL

THIS DOCUMENT IS PROVIDED ON AN "AS IS" BASIS AND DOES NOT IMPLY ANY KIND OF GUARANTEE OR WARRANTY, INCLUDING THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR USE. YOUR USE OF THE INFORMATION ON THE DOCUMENT OR MATERIALS LINKED FROM THE DOCUMENT IS AT YOUR OWN RISK. CISCO RESERVES THE RIGHT TO CHANGE OR UPDATE THIS DOCUMENT AT ANY TIME.

A stand-alone copy or Paraphrase of the text of this document that omits the distribution URL in the following section is an uncontrolled copy, and may lack important information or contain factual errors.

Distribution

This notice will be posted on Cisco's Worldwide Web site at <http://www.cisco.com/warp/public/707/cisco-sa-20020918-smb-dos.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 the following e-mail and Usenet news recipients:

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

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

Revision History

Revision 1.1	2002-September-20	Removed URT from 'fixed' list, reworded summary to more closely match the original Microsoft bulletin
Revision 1.0	2002-September-18	Initial public release

Cisco Security Procedures

Complete information on reporting security vulnerabilities in Cisco products, obtaining assistance with security incidents, and registering to receive security information from Cisco, is available on Cisco's worldwide website at http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html. This includes instructions for press inquiries regarding Cisco security notices. All Cisco security advisories are available at <http://www.cisco.com/go/psirt>.

