Cisco Security Advisory

Microsoft Windows SMB Denial of Service Vulnerabilities in Cisco Products - MS02-045

Severity

Advisory ID: cisco-sa-20020918-smb-dos
Published: 2002 September 18 16:00 GMT
Version1.1: Final
Workarounds: See below

CVE-2002-0724
CWE-119

Download CVRF

Download PDF

Email

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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20020918-smb-dos.

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.

Workarounds

Microsoft documents several workarounds in their bulletin MS02-045.

Fixed Software

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 forward into all later versions
Version 3.0.x	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 forward into all later versions
Version 1.x	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.

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.

Cisco Security Vulnerability Policy

To learn about Cisco security vulnerability disclosure policies and publications, see the Security Vulnerability Policy. This document also contains instructions for obtaining fixed software and receiving security vulnerability information from Cisco.

Related Resources

IS Microsoft Server Message Block Denial of Service Vulnerability

ST 2101

ST 2102

ST 5716

ST 5717

ST 5718

ST 5719

ST 5720

ST 5721

ST 5722

ST 5723

ST 5724

ST 5725

ST 5726

IPS Netbios Enum Share DoS

IPS NetBIOS Enum Share DoS

Show All 16...

Subscribe to Cisco Security Notifications

Subscribe

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20020918-smb-dos

---

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

Legal Disclaimer