Cisco Security Advisory

Microsoft IIS Vulnerabilities in Cisco Products - MS02-018

Severity

Advisory ID: cisco-sa-20020415-ms02-018
Published: 2002 April 15 18:00 GMT
Version1.1: Final
Workarounds: See below

CVE-2002-0071
CVE-2002-0072
CVE-2002-0073
CVE-2002-0074
CVE-2002-0075
CVE-2002-0079
CVE-2002-0147
CVE-2002-0148
CVE-2002-0149
CVE-2002-0150
CVE-2002-0364

Download CVRF
Download PDF
Email

Summary

This advisory describes a vulnerability that affects Cisco products and applications that are installed on Microsoft operating systems incorporating the use of the Internet Information Server (IIS), and is based on the vulnerability of IIS, not due to a defect of the Cisco product or application.

A number of vulnerabilities were discovered that enables an attacker to execute arbitrary code or perform a denial of service against the server. These vulnerabilities were discovered and publicly announced by Microsoft in their Microsoft Security Bulletin MS02-018.

This advisory is available at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20020415-ms02-018.

Affected Products

This section provides details on affected products.

Vulnerable Products

All Cisco products and applications that are using Microsoft IIS are considered vulnerable.

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 3.0, 3.1, 3.2
- Cisco ICS 7750
- Cisco Unity
- Cisco Building Broadband Service Manager 4.x, 5.x
- Cisco uOne Enterprise Edition
- Cisco Network Registrar (CNR)
- Cisco Intelligent Contact Manager (ICM)

The following Cisco products may be installed on various web servers and are vulnerable if installed on a Microsoft IIS server:

- Cisco Collaboration Server (CCS)
- Cisco Dynamic Content Adapter (DCA)
- Cisco Media Blender (CMB)
- TrailHead (Part of the Web Gateway solution)

Various Cisco Network Management products may be installed on Microsoft platforms that may be running a vulnerable version of IIS. Much older versions of CiscoWorks 2000 RWAN/CWSI Campus v2.x and Cisco Voice Manager v1.x are directly vulnerable because IIS was required as a part of the installation. Such systems might be offering HTTP services on default ports. These specific software packages are no longer supported, but are included in this notice to alert customers who might still be using them.

Products Confirmed Not Vulnerable

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

Details

Implementations of the Microsoft Internet Information Server are vulnerable to buffer overflows and denial of service attacks. These vulnerabilities can be exploited to execute arbitrary code on a computer system or to disrupt normal operation of the server.

The vulnerabilities have been described in more detail at http://www.microsoft.com/technet/security/Bulletin/MS02-018.mspx.

Workarounds

Cisco is not aware of any available workarounds for these vulnerabilities and strongly suggests the application of the recommended patches.

Fixed Software

When considering software upgrades, also consult http://www.cisco.com/go/psirt and any subsequent advisories to determine exposure and a complete upgrade solution.

In all cases, customers should exercise caution to be certain the devices to be upgraded contain sufficient memory and that current hardware and software configurations will continue to be supported properly by the new release. If the information is not clear, contact the Cisco Technical Assistance Center ("TAC") or your contracted maintenance provider for assistance.

Cisco CallManager

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

Cisco Unity

Version Affected	**Fixed Regular Release (available now) Fix carries forward into all later versions**
All versions	Install patch for MS02-018

Cisco Building Broadband Service Manager

Version Affected	**Fixed Regular Release (available now) Fix carries forward into all later versions**
Version 4.x	Install patch for MS02-018
Version 5.x	Install patch for MS02-018

Cisco Intelligent Contact Manager

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 IIS Multiple Vulnerabilities

ST 1618

ST 1619

ST 1768

ST 1777

ST 1778

ST 1801

ST 1802

ST 1803

ST 1804

ST 1806

ST 1807

ST 1809

ST 17410

ST 31405

IPS Define Tranfer-Encoding Chunked

IPS finger CGI Recon

IPS HTTP 1.1 Chunked Encoding Transfer

IPS IIS ASP SSI Buffer Overflow

IPS IIS FTP STAT Denial of Service

IPS IIS FTP STAT Denial of Service

IPS IIS HTR ISAPI Buffer Overflow

IPS IIS ISAPI Filter Buffer Overflow

IPS Malformed URL

IPS URL with XSS

IPS WWW finger attempt

IPS WWW finger attempt

Show All 27...

Subscribe to Cisco Security Notifications

Subscribe

Version Affected	Fixed Regular Release (available now) Fix carries forward into all later versions
All versions	Install patch for MS02-018

Exploitation and Public Announcements

The Cisco PSIRT is not aware of any malicious use of the vulnerabilities described in this advisory. The vulnerabilities described here have been discussed publicly on mailing lists and via security advisories released by other sources.

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20020415-ms02-018

Revision History

Revision 1.1	2002-April-16	Removed Cisco E-mail Manager from Affected Products, added fixes for Cisco ICM.
Revision 1.0	2002-April-15	Initial public release
