

# Cisco Security Advisory: Microsoft IIS Vulnerabilities in Cisco Products – MS02–018

Document ID: 46347

Advisory ID: cisco-sa-20020415-ms02-018

<http://www.cisco.com/warp/public/707/cisco-sa-20020415-ms02-018.shtml>

## Revision 1.1

Last Updated 2002 April 16 1800 UTC (GMT)

For Public Release 2002 April 15 1800 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 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://www.cisco.com/warp/public/707/cisco-sa-20020415-ms02-018.shtml>.

## 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.msp> .

## Impact

By gaining unauthorized access, an attacker can view and modify any part of the operating system accessible with the privileges assigned to the web server user possibly leading to a breach of confidentiality and integrity of the system. By performing a denial of service attack, an attacker can cause a disruption in availability of the web server.

# Software Versions and Fixes

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
Version 3.0	forward into all later versions 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
All versions	carries forward into all later versions Install patch for MS02-018

## Cisco Building Broadband Service Manager

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

## Cisco Intelligent Contact Manager

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

## Workarounds

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

## 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](mailto: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 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.

## 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 advisory will be posted on Cisco's worldwide website at <http://www.cisco.com/warp/public/707/cisco-sa-20020415-ms02-018.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](mailto:cust-security-announce@cisco.com)
- [bugtraq@securityfocus.com](mailto:bugtraq@securityfocus.com)
- [first-teams@first.org](mailto:first-teams@first.org) (includes CERT/CC)
- [cisco@spot.colorado.edu](mailto:cisco@spot.colorado.edu)
- [comp.dcom.sys.cisco](mailto:comp.dcom.sys.cisco)
- [firewalls@lists.gnac.com](mailto:firewalls@lists.gnac.com)
- Various internal Cisco mailing lists

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

## 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

## 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 Web site at [http://www.cisco.com/en/US/products/products\\_security\\_vulnerability\\_policy.html](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>.

---

All contents are Copyright © 2006–2007 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

---

Updated: Apr 16, 2002

Document ID: 46347

---