

Cisco Security Advisory: Cisco Wireless Control System Tomcat mod_jk.so Vulnerability

Advisory ID: cisco-sa-20080130-wcs

<http://www.cisco.com/warp/public/707/cisco-sa-20080130-wcs.shtml>

Revision 1.1

Last Updated 2008 April 25 2000 UTC (GMT)

For Public Release 2008 January 30 1600 UTC (GMT)

Please provide your [feedback](#) on this document.

Contents

[Summary](#)

[Affected Products](#)

[Details](#)

[Vulnerability Scoring 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

Apache Tomcat is the servlet container for JavaServlet and JavaServer Pages Web within the Cisco Wireless Control System (WCS). A vulnerability exists in the mod_jk.so URI handler within Apache Tomcat which, if exploited, may result in a remote code execution attack.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20080130-wcs.shtml>.

[\[Expand all sections\]](#) [\[Collapse all sections\]](#)

☐ Affected Products

This section provides details on affected products.

☐ Vulnerable Products

Cisco WCS devices running software 3.x and 4.0.x prior to 4.0.100.0 are affected by this vulnerability. Cisco WCS devices running software 4.1.x and 4.2.x prior to to version 4.2.62.0 are also vulnerable.

Note: The version of WCS software installed on a particular device can be found via the WCS HTTP management interface. Select **Help -> About the Software** to obtain the software version.

☐ Products Confirmed Not Vulnerable

No other Cisco products are currently known to be affected by this vulnerability.

[Top of the section](#) [Close Section](#)

☐ Details

The Cisco Wireless Control System is a centralized, systems-level platform for managing and controlling lightweight access points, wireless LAN controllers, and Wireless Location Appliances for the Cisco Unified Wireless Network. The Cisco Wireless Control System uses Apache Tomcat. A vulnerability in Apache Tomcat may allow for remote code execution attacks. The mod_jk.so

URI handler does not handle long URLs correctly. An insecure memory copy triggers an exploitable stack overflow. This vulnerability is documented in [CVE-2007-0774](#) and in Cisco bug ID [CSCsk18191](#) ([registered](#) customers only) .

[Top of the section](#) [Close Section](#)

☐ Vulnerability Scoring Details

Cisco has provided scores for the vulnerability in this advisory based on the Common Vulnerability Scoring System (CVSS). The CVSS scoring in this Security Advisory is done in accordance with CVSS version 2.0.

CVSS is a standards-based scoring method that conveys vulnerability severity and helps determine urgency and priority of response.

Cisco has provided a base and temporal score. Customers can then compute environmental scores to assist in determining the impact of the vulnerability in individual networks.

Cisco has provided an FAQ to answer additional questions regarding CVSS at

<http://www.cisco.com/web/about/security/intelligence/cvss-qandas.html>.

Cisco has also provided a CVSS calculator to help compute the environmental impact for individual networks at

<http://intellishield.cisco.com/security/alertmanager/cvss>.

CSCsk18191 - WCS mod_jk.so Apache Tomcat vulnerability					
Calculate the environmental score of CSCsk18191					
CVSS Base Score - 10.0					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	Complete	Complete	Complete
CVSS Temporal Score - 8.3					
Exploitability		Remediation Level		Report Confidence	

Functional	Official-Fix	Confirmed
------------	--------------	-----------

[Top of the section](#) [Close Section](#)

☐ Impact

Successful exploitation of the vulnerability may result in remote code execution.

[Top of the section](#) [Close Section](#)

☐ Software Versions and Fixes

Each row of the following software table (below) describes a release train and the platforms or products for which it is intended. If a given release train is vulnerable, then the earliest possible releases that contain the fix are shown in the "First Fixed Release" column. A device running a release in the given train that is earlier than the release in a specific column (less than the First Fixed Release) is known to be vulnerable. The release should be upgraded at least to the indicated release or a later version (greater than or equal to the First Fixed Release label).

Affected Releases	First Fixed Releases
WCS for Linux and Windows 4.0.x and earlier	4.0.100.0
WCS for Linux and Windows 4.1.91.0 and earlier	4.2.62.0

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.

[Top of the section](#) [Close Section](#)

☐ Workarounds

The following workarounds can be implemented.

Transit ACLs (tACL)

Filters that deny HTTPS packets using TCP port 443 should be deployed throughout the network as part of a tACL policy for protection of traffic which enters the network at ingress access points. This policy should be configured to protect the network device where the filter is applied and other devices behind it. Filters for HTTPS packets using TCP port 443 should also be deployed in front of vulnerable network devices so that traffic is only allowed from trusted clients.

Additional information about tACLs is available in "Transit Access Control Lists: Filtering at Your Edge":

http://www.cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a00801afc76.shtml

Additional Mitigation Techniques

Additional mitigation techniques that can be deployed on Cisco devices within the network are available in the Cisco Applied Intelligence companion document for this advisory:

<http://www.cisco.com/warp/public/707/cisco-amb-20080130-wcs.shtml>

[Top of the section](#) [Close Section](#)

☐ Obtaining Fixed Software

Cisco has released free software updates that address this vulnerability. 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/en/US/docs/general/warranty/English/EU1KEN_.html, or as otherwise set forth at Cisco.com Downloads at <http://www.cisco.com/public/sw-center/sw-usingswc.shtml>.

Do not contact 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 agreements 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 do not hold a Cisco service contract, and customers who purchase through third-party vendors but are unsuccessful in obtaining fixed software through their point of sale should acquire 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

Customers should have their product serial number available and be prepared to give the URL of this notice as evidence of 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 localized telephone numbers, and instructions and e-mail addresses for use in various languages.

[Top of the section](#) [Close Section](#)

☐ Exploitation and Public Announcements

The Cisco PSIRT is aware of the availability of proof-of-concept exploits.

[Top of the section](#) [Close Section](#)

☐ **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.

[Top of the section](#) [Close Section](#)

☐ **Distribution**

This advisory is posted on Cisco's worldwide website at:

<http://www.cisco.com/warp/public/707/cisco-sa-20080130-wcs.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
- first-teams@first.org
- bugtraq@securityfocus.com
- vulnwatch@vulnwatch.org
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- full-disclosure@lists.grok.org.uk
- comp.dcom.sys.cisco@newsgate.cisco.com

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	2008-April-25	Updated CVSS link for CSCsk18191 .
Revision 1.0	2008-January-30	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>.

Help us help you.

☐ Please rate this document.

- Excellent
- Good
- Average
- Fair
- Poor

☐ This document solved my problem.

- Yes
- No
- Just browsing

Suggestions for improvement:

(256 character limit)



[Home](#)

[How to Buy](#)

[Login](#)

[Profile](#)

[Feedback](#)

[Site Map](#)

[Help](#)

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 - 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) |

[Trademarks of Cisco Systems, Inc.](#)