

# Cisco Security Advisory: Cisco Collaboration Server Vulnerability

Document ID: 59687

Advisory ID: cisco-sa-20040630-CCS

<http://www.cisco.com/warp/public/707/cisco-sa-20040630-CCS.shtml>

## Revision 1.0

For Public Release 2004 June 30 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

Cisco Collaboration Server (CCS) versions earlier than 5.0 ship with ServletExec versions that are vulnerable to attack where unauthorized users can upload any file and gain administrative privileges. The workaround is documented in the Workaround section below. Cisco has provided an automated script to remove this vulnerability from the CCS 4.x versions

This advisory is available at <http://www.cisco.com/warp/public/707/cisco-sa-20040630-CCS.shtml>.

## Affected Products

This section provides details on affected products.

### Vulnerable Products

CCS using an unpatched ServletExec version earlier than 3.0E is vulnerable.

- CCS 4.x ships with ServletExec 3.0 which is vulnerable until patched. CCS 4.0 customers can patch the software with an automated script or upgrade to CCS 5.x.
- CCS 3.x ships with ServletExec 2.2 which is vulnerable until patched. An automated script is not available for CCS 3.0. Customers can patch the software by following the manual instructions in the

Workaround section, upgrade to CCS 4.x and patch the software with an automated script, or upgrade to CCS 5.x.

## Products Confirmed Not Vulnerable

CCS 5.x ships with ServletExec 4.1 and is not vulnerable.

## Details

Cisco Collaboration Server utilizes the ServletExec subcomponent provided by New Atlanta for Microsoft Windows 2000 and Windows NT. ServletExec versions prior to SE 3.0E allow for an attacker to upload files to the Web server and invoke them. Cisco bug id CSCed49648. Users should either upgrade to CCS 5.x which ships with ServletExec 4.1, download the automated script for CCS 4.x, or follow the manual instructions in the Workaround section.

Patching ServletExec either with the automated script or manual instructions removes the UploadServlet from the ServletExec30.jar file but does not alter the version number. The best way to test if the CCS is vulnerable is to attempt to load the `http://<ccsservername>/servlet/UploadServlet` URL when CCS is up and running. If this attempt results in a `NullPointerException`, the vulnerability is present. If this results in a Page Not Found error, then the CCS is not vulnerable.

Customers can continue to obtain and apply the most current patches for ServletExec by following the instructions on the New Atlanta website:

[http://www.newatlanta.com/biz/c/products/servletexec/self\\_help/faq/detail?faqId=195](http://www.newatlanta.com/biz/c/products/servletexec/self_help/faq/detail?faqId=195) . Additionally, customers are encouraged to go to the following Cisco web pages for tips on increasing security on their CCS: [http://www.cisco.com/en/US/docs/voice\\_ip\\_comm/cust\\_contact/contact\\_center/ipcc\\_enterprise/srnd/7x/c7scurty.html](http://www.cisco.com/en/US/docs/voice_ip_comm/cust_contact/contact_center/ipcc_enterprise/srnd/7x/c7scurty.html) Refer to page 38 for ServletExec notes and refer to page 71 for notes on Collaboration Option.

Cisco Collaboration Server (CCS) has been sold as a standalone product or as part of Cisco Web Collaboration Option where it is integrated with the Cisco Intelligent Contact Management (ICM) software. A user can determine their version level by using the `http://<ccs server>/version` command, where `<ccs server>` is the hostname or IP address.

## Impact

Cisco Collaboration Server (CCS) versions earlier than 5.0 ship with ServletExec versions that are vulnerable to attack where unauthorized users can upload any file and gain administrative privileges.

- [CSCed49648](#)

## Software Versions and Fixes

Cisco Collaboration Server 4.x users can patch the software with an automated script available at <http://www.cisco.com/cgi-bin/tablebuild.pl/ccs40>, or patch the software by following the manual instructions in the Workaround section, or upgrade to CCS 5.x.

Cisco Collaboration Server 3.x users can patch the software by following the manual instructions in the Workaround section, or upgrade to CCS 4.x and patch the software with an automated script, or upgrade to CCS 5.x.

# Workarounds

## Manual Instructions to Patch CCS 3.x

Complete these steps to patch CCS 3.x:

1. Stop Internet Information Server (IIS).
2. Run Winzip or your favorite zip utility and open ServletExec22.jar in the C:\Program Files\new atlanta\servletexec ISAPI\lib directory.
3. Delete UploadServlet.class.
4. Save ServletExec22.jar back to its original location and exit Winzip.
5. Restart IIS.

## Manual Instructions to Patch CCS 4.x

Complete these steps to patch CCS 4.x:

1. Stop Internet Information Server (IIS).
2. Run Winzip or your favorite zip utility and open ServletExec30.jar in the C:\Program Files\new atlanta\servletexec ISAPI\lib directory.
3. Delete UploadServlet.class.
4. Save ServletExec30.jar back to its original location and exit Winzip.
5. Restart IIS.

CCS 5.x is not vulnerable and these manual instructions do not apply.

## 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 public announcements or malicious use of the vulnerability described in this advisory. We would like to thank Matt Moore of Pentest Limited for finding and reporting this vulnerability to us.

## 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 is posted on Cisco's worldwide website at <http://www.cisco.com/warp/public/707/cisco-sa-20040630-CCS.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)
- [first-teams@first.org](mailto:first-teams@first.org) (includes CERT/CC)
- [bugtraq@securityfocus.com](mailto:bugtraq@securityfocus.com)
- [vulnwatch@vulnwatch.org](mailto:vulnwatch@vulnwatch.org)

- [cisco@spot.colorado.edu](mailto:cisco@spot.colorado.edu)
- [cisco-nsp@puck.nether.net](mailto:cisco-nsp@puck.nether.net)
- [full-disclosure@lists.netsys.com](mailto:full-disclosure@lists.netsys.com)
- [comp.dcom.sys.cisco@newsgate.cisco.com](mailto: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 1.0	2004-June-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](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>.

---

[Contacts & Feedback](#) | [Help](#) | [Site Map](#) © 2007 – 2008 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

---

Updated: Jun 30, 2004

Document ID: 59687

---