

Cisco Security Advisory: CDS Internet Streamer: Web Server Directory Traversal Vulnerability

Advisory ID: **cisco-sa-20100721-spcdn**

<http://www.cisco.com/warp/public/707/cisco-sa-20100721-spcdn.shtml>

Revision 1.1

Last Updated 2010 July 29 1300 UTC (GMT)

For Public Release 2010 July 21 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

The Cisco Internet Streamer application, part of the Cisco Content Delivery System, contains a directory traversal vulnerability on its web server component that allows for arbitrary file access. By exploiting

this vulnerability, an attacker may be able to read arbitrary files on the device, outside of the web server document directory, by using a specially crafted URL.

An unauthenticated attacker may be able to exploit this issue to access sensitive information, including the password files and system logs, which could be leveraged to launch subsequent attacks.

Cisco has released free software updates that address this vulnerability.

Workarounds that mitigate this vulnerability are available.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20100721-spcdn.shtml>.

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

☐ Affected Products

All versions of system software on the Cisco Internet Streamer application are vulnerable prior to the first fixed release.

☐ Vulnerable Products

To determine the software version running on a Cisco Content Delivery Engine, log in to the device and issue the "**show version**" command line interface (CLI) command to display the system banner. Cisco CDS Internet Streamer software will identify itself as "Content Delivery System Software Release". On the same line of output, the version number will be provided. This example identifies a Cisco Content Delivery Engine that is running Cisco Content Delivery System software release 2.5.3:

```
cdn-cde#show version
Content Delivery System Software (CDS)
Copyright ©) 1999-2010 by Cisco Systems, Inc.
Content Delivery System Software Release 2.5.3 (build b8 Jan 21 2010)
Version: cde200-2.5.3.8

Compiled 16:07:11 Jan 21 2010 by ipvbuild
Compile Time Options: KQ SS

System was restarted on Thu Jun  3 04:09:25 2010.
The system has been up for 2 hours, 11 minutes, 27 seconds.

cdn-cde#
```

Alternatively the Content Delivery System Manager home page gives a brief summary of the software versions in use on all the devices in the content delivery system network.

To view the software version running on a particular device, choose Devices > Devices. The Devices Table page displays the software version for each device listed. For further information on finding the software version, refer to the "Maintaining the Internet Streamer CDS" at the following link:

http://www.cisco.com/en/US/docs/video/cds/cda/is/2_5/configuration_guide/maint.html#wp1198510.

☐ Products Confirmed Not Vulnerable

Cisco Content Delivery Engines running TV streaming content delivery applications and the Video Navigator Application are not affected.

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

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

☐ Details

The Cisco Internet Streamer application provides edge caching, content streaming, and downloads to subscriber IP devices such as PCs.

The Cisco Internet Streamer application, part of the Cisco Content Delivery System, contains a directory traversal vulnerability on its web server component that allows for arbitrary file access. It is possible to read arbitrary files on the Cisco Content Delivery Engine running the internet streamer application outside the web server's document directory using a specially-crafted URL. This includes the password files used to hold admin account details and system logs.

An unauthenticated attacker may be able to exploit this issue to access sensitive information that could be leveraged to launch subsequent attacks.

On the Service Engine and the Cisco Content Delivery System Manager this vulnerability can be exploited over all open HTTP ports; TCP ports 80 (Default HTTP port), 443 (Default HTTPS port) and 8090 (Alternate HTTP and HTTPS port), as well as those that are configured as part of the HTTP proxy.

On the Service Router this issue is seen on port TCP port 8090 (Alternate HTTP and HTTPS port).

In Cisco content delivery system software 2.5.3 and earlier, it is possible to configure "Enable Incoming Proxy", which when enabled, accepts incoming requests on configured ports, in addition to TCP port 80. The additional ports that the device will listen on for HTTP requests is defined in the "List of Incoming HTTP Ports" field, within "Devices > Devices > Application Control > Web > HTTP > HTTP Connections" of the content delivery system manager menu. For further information on HTTP settings, refer to the "Cisco Internet Streamer CDS 2.5 Software Configuration Guide - Configuring Devices" at the following link:

http://www.cisco.com/en/US/docs/video/cds/cda/is/2_5/configuration_guide/configdevice.html.

This vulnerability is documented in the Cisco Bug ID [CSCtd68063](#) ([registered](#) customers only) and has been assigned Common Vulnerabilities and Exposures (CVE) ID CVE-2010-1577.

[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>.

| CSCtd68063: CDS Internet Streamer: Web Server Directory Traversal Vulnerability. | | | | | |
|---|-------------------|-------------------|------------------------|-------------------|---------------------|
| Calculate the environmental score of CSCtd68063 | | | | | |
| CVSS Base Score - 7.8 | | | | | |
| Access Vector | Access Complexity | Authentication | Confidentiality Impact | Integrity Impact | Availability Impact |
| Network | Low | None | Complete | None | None |
| CVSS Temporal Score - 6.4 | | | | | |
| Exploitability | | Remediation Level | | Report Confidence | |
| Functional | | Official-Fix | | Confirmed | |

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

☐ Impact

An unauthenticated attacker may be able to exploit this issue to access sensitive information, including the password files and system logs, which could be leveraged to launch subsequent attacks.

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

☐ 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.

The recommended release contains other software fixes that are recommended by Cisco. For further information please consult the release notes at the following link:

http://www.cisco.com/en/US/docs/video/cds/cda/is/2_5/release_notes/CDS_RelNotes2_5_9.html#wp100128

| Cisco Content Delivery System Software Release | First Fixed Release | Recommended Release |
|--|---|---------------------|
| 2.2.x | Vulnerable, Migrate to 2.5.7 or later | |
| 2.3.x | Vulnerable, Migrate to 2.5.7 or later | |
| 2.4.x | Vulnerable, Migrate to 2.5.7 or later | |
| 2.5.x | 2.5.7 | 2.5.9 |

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

Workarounds

Service Rules

As an interim step prior to upgrading the Cisco content delivery system software, it is possible to deny access to sensitive directories via service rules. This workaround is applicable to the Service Engine only. The following example shows denying access to move up a directory level. This also caters for other directory moves, such as "\.\/", "\.\/" or "\.\/":

```
rule enable
rule action block pattern-list 1
rule pattern-list 1 url-regex ^http://.*/*/*.*
rule pattern-list 1 url-regex ^https://.*/*/*.*
```

For more information on configuring service rules and for instructions on how to perform this via the content delivery system manager, consult the Cisco Internet Streamer CDS 2.5 Software Configuration Guide at the following link:

http://www.cisco.com/en/US/docs/video/cds/cda/is/2_5/configuration_guide/configdevice.html#wp1773573.

Cisco CDS Engine IP Access Control Lists

This workaround is applicable only for the service router and Content Delivery System Manager, which do not have support for the above service rules. It is not applicable to the service engine.

Although it is often difficult to block traffic that transits a network, it is possible to identify traffic that should never be allowed to target infrastructure devices and block that traffic at the interface of the device or at the border of networks. The IP ACL example below provides an example of a trusted network segment 192.168.10.X that is allowed HTTP access (on TCP ports 80 and 443) to the Cisco content delivery service engine interface IP address 10.1.1.1. All other HTTP traffic to this address is dropped.

Note: The IP ACL should include all the configured interface IP addresses on the Cisco content delivery service engine. In this example only one interface IP address is shown:

```
ip access-list extended cisco-sa-20100721-spcdn
  permit tcp 192.168.10.0 0.0.0.255 host 10.1.1.1 eq www
  permit tcp 192.168.10.0 0.0.0.255 host 10.1.1.1 eq https

!--
!-- TCP port 8090 is not normally used so normally will not have to
!-- be explicitly permitted.
!--
!-- Permit any additional TCP ports that may have been configured
!-- via the HTTP Proxy before continuing to add the deny statements.
!--

deny tcp any host 10.1.1.1 eq 8090
deny tcp any host 10.1.1.1 eq www
deny tcp any host 10.1.1.1 eq https
permit ip any any
exit
```

Apply the IP ACL to all interfaces on the Cisco content delivery service router or Content Delivery System Manager. In this example only one interface is shown:

```
interface GigabitEthernet 2/0
  ip address 10.1.1.1 255.255.255.0
  ip access-group cisco-sa-20100721-spcdn in
```

For more information on configuring IP access-lists and for instructions on how to perform this via the content delivery system manager, consult the Cisco Internet Streamer CDS 2.5 Software Configuration Guide at the following link:

http://www.cisco.com/en/US/docs/video/cds/cda/is/2_5/configuration_guide/configdevice.html#wpl086184

[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/en/US/support/tsd_cisco_worldwide_contacts.html 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 not aware of any public announcements or malicious use of the vulnerability described in this advisory.

This vulnerability was reported to Cisco by BT and identified by Christopher Richardson & Simon John.

[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-20100721-spcdn.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-bulletins@lists.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.

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

☐ **Revision History**

| | | |
|-----------------|-----------------|--|
| Revision 1.1 | 2010 July 29 | Updated Details and Workaround sections |
|-----------------|-----------------|--|

| | | |
|-----------------|-----------------|------------------------|
| Revision 1.0 | 2010 July 21 | Initial public release |
|-----------------|-----------------|------------------------|

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

☐ 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>.

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

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](#)

© 2009 - 2010 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)