

Cisco Security Advisory: Cisco Web Cache Control Protocol Router Vulnerability

Document ID: 13668

Advisory ID: cisco-sa-19980513-wccp-auth

<http://www.cisco.com/warp/public/707/cisco-sa-19980513-wccp-auth.shtml>

Revision 1.0

For Public Release 1998 May 13 1500 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's Cisco Cache Engine product provides transparent caching for world-wide web pages retrieved via HTTP. The Cache Engine uses a Cisco proprietary protocol called the Web Cache Control Protocol (WCCP) to communicate with a properly-configured Cisco router and register as a cache service provider. The router then diverts HTTP traffic to the Cache Engine.

Although this process is not enabled by default, and takes place only if a user specifically configures the router to enable WCCP, there is no authentication in WCCP itself. A router configured to support Cache Engines will treat any host that sends it valid WCCP hello packets as a cache engine, and may divert HTTP traffic to that host. This means that it is possible for malicious users to divert web traffic passing through such a router, even though they may not have either physical or configuration access to the router.

This attack can be avoided by using access lists to prevent WCCP traffic from untrusted hosts from reaching the router. Cisco will be modifying WCCP to include hash-based authentication in a future release.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-19980513-wccp-auth.shtml>.

Affected Products

This section provides details on affected products.

Vulnerable Products

All users of the Cisco Cache Engine and WCCP who have not configured filtering access lists to prevent WCCP access by unauthorized hosts are affected by this attack.

Products Confirmed Not Vulnerable

Users who have not specifically configured their routers to enable WCCP are *not* affected by this attack. If the character string "wccp" does not appear in your router configuration file, you are not affected.

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

Details

This vulnerability has been assigned Cisco bug ID [CSCdk07174](#). If you are a [registered](#) CCO user and you have logged in, you can view bug details.

Impact

Attackers can cause a router configured for WCCP to divert some or all HTTP traffic to any host they choose, anywhere on the Internet. Once having done this, attackers are able to:

- intercept confidential information, including site access passwords
- substitute data of their own choosing for the actual content of web pages
- disrupt web service for connections passing through the targeted router

In order to do this, the attacker would either need a Cisco Cache Engine or software capable of generating WCCP traffic. Cisco sells Cache Engines to the general public, although a relatively small number have been shipped thus far. The WCCP protocol specification is unpublished, but the protocol is not immune to reverse engineering.

Software Versions and Fixes

This vulnerability affects all versions of Cisco IOS software that support WCCP that have been released as of the date of this notice. This includes Cisco IOS 11.2(P) releases beginning with 11.2(10)P, 11.1CA releases beginning with 11.1(14)CA, and 11.1 releases derived from 11.1(14)CA, including 11.1CC.

Cisco plans to release software that supports authentication for WCCP. This will involve a modification to the WCCP protocol. In order to take advantage of the authentication features, customers will need to upgrade the software in both routers and Cache Engines, and will need to make some minor configuration changes on both devices. Release of the improved software is tentatively scheduled for September, 1998, but this schedule is subject to change. Cisco believes that the workaround described below will adequately protect Cache Engine users until the new software is ready.

Cisco is considering making an interim fix involving an explicit command to apply an access list to all incoming WCCP traffic. This would be largely equivalent to the workaround discussed below, but might be easier for some users to configure. No decision has been made on when or whether to offer this interim fix. If an interim fix is created, this notice will be updated to reflect that fact.

Workarounds

WCCP runs over UDP at port 2048. By blocking unauthorized UDP traffic destined to port 2048 on the router running WCCP, attackers can be prevented from sending WCCP traffic to the router, and therefore from diverting any actual traffic. For proper security, it's important to block all traffic destined for port 2048 at any address assigned to the router, as well as at all broadcast addresses for networks on which the router may be attached, and all multicast addresses to which the router may be listening. The blocking can be configured either using inbound access lists on the WCCP router itself, or using access lists or other filtering on surrounding devices.

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

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

Cisco has had no reports of malicious exploitation of this vulnerability.

Cisco knows of no public announcements of this vulnerability before the date of this notice. However, the vulnerability has been independently identified by several people both inside and outside of Cisco, and should be considered to be public knowledge.

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

In addition to this CCO version of the field notice, the initial version of this notice is also being sent via e-mail to the following recipients:

- cust-security-announce@cisco.com
- Identified Cisco Cache Engine customers. Cisco does not guarantee its ability to identify every person or organization that may be in possession of a Cache Engine, nor to exclude every person or organization that does not have a Cache Engine.
- bugtraq@netspace.org
- first-teams@first.org (includes CERT/CC)
- 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.

This advisory is posted on Cisco's worldwide website at <http://www.cisco.com/warp/public/707/cisco-sa-19980513-wccp-auth.shtml>.

Revision History

| | | |
|--------------|-------------|--------------------------|
| Revision 1.0 | 1998-MAY-13 | Initial released version |
|--------------|-------------|--------------------------|

Cisco Security Procedures

Please report security issues with Cisco products, and/or sensitive security intrusion emergencies involving Cisco products, to security-alert@cisco.com. Reports may be encrypted using PGP; public RSA and DSS keys for "security-alert@cisco.com" are on the public PGP key servers.

The alias "security-alert@cisco.com" is used only for reports incoming to Cisco. Mail sent to the list goes only to a very small group of users within Cisco. Neither outside users nor unauthorized Cisco employees may subscribe to "security-alert@cisco.com".

Please do not use "security-alert@cisco.com" for configuration questions, for security intrusions that you do not consider to be sensitive emergencies, or for general, non-security-related support requests. We do not have the capacity to handle such requests through this channel, and will refer them to Cisco's Technical Assistance Center (TAC), delaying response to your questions. We advise contacting the TAC directly with these requests:

- (800) 553-24HR
- (408) 526-7209
- e-mail: tac@cisco.com

All formal public security notices generated by Cisco are sent to the public mailing list "cust-security-announce@cisco.com". For information on subscribing to this mailing list, send a message containing the single line "info cust-security-announce" to "majordomo@cisco.com". An analogous list, "cust-security-discuss@cisco.com", is available for public discussion of the notices and of other Cisco security issues.

All contents are Copyright © 2006-2007 Cisco Systems, Inc. All rights reserved. [Important Notices](#) and [Privacy Statement](#).

Updated: May 13, 1998

Document ID: 13668
