

Cisco Security Advisory: Transparent Cache Engine and Content Engine TCP Relay Vulnerability

Document ID: 23663

Advisory ID: cisco-sa-20020515-transparent-cache-tcp-relay

<http://www.cisco.com/warp/public/707/cisco-sa-20020515-transparent-cache-tcp-relay>

Revision 2.0

Last Updated 2004 January 05 1700 UTC (GMT)

For Public Release 2002 May 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

Cisco Cache Engines and Content Engines provide a transparent cache for world wide web pages retrieved via HTTP. These products also can be configured to transparently intercept requests to proxy servers supporting various protocols such as HTTPS. The default configuration of the proxy feature can be abused to open a TCP connection to any reachable destination IP address and hide the true IP source address of the connection. This behavior has been implicated in a variety of undesirable and possibly illegal activities such as transmitting unsolicited commercial e-mail, unauthorized network scanning, and denial of service attacks.

There are two vulnerabilities that may cause this problem.

- The vulnerability for the HTTP proxy can be resolved by upgrading the code to a fixed version.
- The vulnerability for the HTTPS proxy can be resolved in the field by changing the configuration of the affected device.

Fixed versions of the software have been modified to provide a more secure configuration by default.

Cisco Security Advisory: Transparent Cache Engine and Content Engine TCP Relay Vulnerability

This advisory is available at
<http://www.cisco.com/warp/public/707/cisco-sa-20020515-transparent-cache-tcp-relay.shtml> .

Affected Products

This section provides details on affected products.

Vulnerable Products

The following Cisco Cache Engine and Content Engine products are affected if they are running the specified versions of software:

- Content Engine 507, 510, 560, 565, 590, 7305, 7320 or 7325 running cache software 2.x, 3.1, 4.0.x, 4.1.x, 4.2.x, 5.0.x, 5.1.x
- Cache Engine 505, 550, or 570 running software version 2.2.0 or above
- Content Router CR-4430 running ACNS 4.x
- Content Distribution Manager CDM-4630 or CDM-4650 running ACNS 4.x
- Content Engine Module for Cisco Routers 2600, 3600 and 3700

Products Confirmed Not Vulnerable

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

Details

The vulnerability for the HTTPS proxy has been assigned Cisco bug ID CSCdx05705, which modifies the default settings to ensure the administrator must specify permitted traffic.

The ability to handle proxied requests was added in version 2.2.0 of the Cache Engine software. More details are provided in the Release Notes at http://www.cisco.com/univercd/cc/td/doc/product/webscale/webcache/rn_ce220.htm#xtocid71711.

In addition to caching pages from remote web servers, the cache software also has the ability to cache data for other proxy servers using a variety of supported protocols such as FTP and HTTPS. This function is enabled by default. Since proxied HTTPS services may be available on a variety of ports, the device can be instructed by a client to open a TCP connection to any reachable IP address and port.

The following warning is displayed during configuration and the boot process when the Cache Engine running version 2.x is configured as an HTTPS proxy server without transparent redirection:

It is recommended to set restrictions that allow or deny HTTPS traffic to Destination Ports. Default settings may not provide the desired security level.

This warning is not displayed when the device operated in transparent mode and is not shown in any case when running software versions 3.x and 4.x.

This issue has been resolved by changing the default behavior when HTTPS proxy is enabled so that connections are limited based on the destination port numbers and connections to ports less than 1024 (excluding 443 and 563) are denied.

The vulnerability for the HTTP proxy has been assigned Cisco bug ID CSCeb19815, which introduces the new "http destination-port <deny|allow> <all|port ranges>" command and modifies the default settings to ensure the administrator must specify permitted traffic.

The HTTP proxy vulnerability has been resolved by changing the default behavior so that the HTTP connections are limited based on the destination port numbers and connections to reserved ports (1–79 and 88–1024) are denied.

Impact

Cisco Cache Engines and Content Engines can be used to forward unexpected traffic, and to obscure the true originator of undesirable traffic.

Software Versions and Fixes

The vulnerability for the HTTP proxy can be corrected by customers by upgrading to ACNS 4.2(11.3), 5.0(5.2) and 5.1(0.190). A new command has been introduced in these versions to control HTTP destinations ports and the default configuration has been corrected.

The vulnerability for HTTPS proxy can be corrected by customers in the field by modifying the configuration of the device. A software upgrade is not required to address the HTTPS vulnerability.

The default behavior for both vulnerabilities are corrected in ACNS 4.2(11.3), 5.0(5.2), 5.1(0.190) and will be carried forward into all future versions.

Workarounds

There is no workaround for the HTTP proxy vulnerability below 4.2(11.3), 5.0(5.2) and 5.1(0.190). The default behavior has been changed in these versions, so no other configuration is needed for these versions and above.

The problem for the HTTPS proxy can be solved by a configuration command, which blocks the use of redirected proxy requests for any port other than 443.

```
https destination-port allow 443
https destination-port deny all
```

If the HTTPS proxy is not necessary to an installation, then the command "https destination-port allow 443" can be excluded from the above workaround.

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

The Cisco PSIRT is aware of several instances in which Cisco Cache Engines or Content Engines have been abused to transmit unsolicited commercial e-mail and hide the true source of the message.

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.

Cisco Security Advisory: Transparent Cache Engine and Content Engine TCP Relay Vulnerability

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-20020515-transparent-cache-tcp-relay.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
- bugtraq@securityfocus.com
- first-teams@first.org (includes CERT/CC)
- cisco@spot.colorado.edu
- comp.dcom.sys.cisco
- 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 2.0 | 2004-Jan-05 | Added the HTTP vulnerability (CSCeb19815). Updated the Summary, Details, Fixed Software and Workarounds sections. |
| Revision 1.1 | 2002-May-28 | Updated Details section. |
| Revision 1.0 | 2002-May-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 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>.

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

Updated: Jan 05, 2004

Document ID: 23663
