

[NEWS] Transparent Cache Engine and Content Engine TCP Relay Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-05/0074.html>

From: support@securiteam.com

Date: 05/18/02

From: support@securiteam.com

To: list@securiteam.com

Date: Sat, 18 May 2002 22:41:18 +0200 (CEST)

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

Transparent Cache Engine and Content Engine TCP Relay Vulnerability

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.

This vulnerability 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.

DETAILS

Affected Products:

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

Securiteam: [NEWS] Transparent Cache Engine and Content Engine TCP Relay Vulnerability

- * Content Engine 507, 560, 590, or 7320 running cache software 2.x, 3.1, 4.0.x, or 4.1.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

No other Cisco products are affected by this vulnerability.

Details:

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 <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 are denied.

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

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:

This vulnerability can be corrected by customers in the field by modifying the configuration of the device. A software upgrade is not required to address this vulnerability.

The default behavior is corrected in version ACNS 4.1(3.3) and will be carried forward into all future versions.

Securiteam: [NEWS] Transparent Cache Engine and Content Engine TCP Relay Vulnerability

Cache Engines CE-505, 550 and 570 cannot be upgraded to ACNS version 4.1 software, and thus only the configuration workaround will apply.

Obtaining Fixed Software:

Cisco is offering free software upgrades for systems that can run ACNS software version 4.1. The software upgrade is equivalent to manually changing the default behavior in the device's configuration and thus corrected software is not available for older or unsupported releases. Customers may only install and expect support for the feature sets they have purchased.

Customers with service contracts should contact their regular update channels to obtain the free software upgrade identified via this advisory. For most customers with service contracts, this means that upgrades should be obtained through the Software Center on Cisco's Worldwide Web site at <http://www.cisco.com>.

Customers whose Cisco products are provided or maintained through a prior or existing agreement with third-party support organizations such as Cisco Partners, authorized resellers, or service providers should contact that support organization for assistance with obtaining the free software upgrade(s).

Customers who purchased directly 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 obtain fixed software by contacting the Cisco Technical Assistance Center (TAC) using the contact information listed below. In these cases, customers are entitled to obtain an upgrade to a later version of the same release or as indicated by the applicable corrected software version in the Software Versions and Fixes section (noted above).

Cisco 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

See <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.

Please have your product serial number available and give the URL of this notice as evidence of your entitlement to a free upgrade.

Please do not contact either "psirt@cisco.com" or "security-alert@cisco.com" for software upgrades.

Workarounds:

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

Securiteam: [NEWS] Transparent Cache Engine and Content Engine TCP Relay Vulnerability

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.

ADDITIONAL INFORMATION

The information has been provided by <mailto:psirt@cisco.com> Cisco Systems Product Security Incident Response Team.

=====

This bulletin is sent to members of the SecuriTeam mailing list.
To unsubscribe from the list, send mail with an empty subject line and body to:
list-unsubscribe@securiteam.com
In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====
=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.
In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.

-
- **Previous message:** support@securiteam.com: "[NT] Opera JavaScript Protocol Vulnerability"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)