

Cisco Security Advisory: Cisco VPN 3000 Concentrator Vulnerable to Crafted HTTP Attack

Document ID: 68869

Advisory ID: cisco-sa-20060126-vpn

<http://www.cisco.com/warp/public/707/cisco-sa-20060126-vpn.shtml>

Revision 2.1

Last Updated 2007 August 14 1600 UTC (GMT)

For Public Release 2006 January 26 1700 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

The Cisco VPN 3000 series concentrators are a family of purpose-built, remote access Virtual Private Network (VPN) platforms for data encryption and authentication.

A malicious user may be able to send crafted packets to a concentrator which may cause the device to halt and/or drop user connections. The power must then be reset on the device to recover.

Cisco has made free software available to address this vulnerability for affected customers. There are workarounds available to mitigate this vulnerability as well.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20060126-vpn.shtml>.

Affected Products

This section provides details on affected products.

Vulnerable Products

Cisco VPN 3000 series concentrators 3005, 3015, 3020, 3030 and the 3080 are affected by this vulnerability.

Products Confirmed Not Vulnerable

The following products are confirmed not vulnerable:

- Cisco VPN 3002 Hardware Client
- Cisco IPSec VPN Services Module (VPNSM)
- Cisco WebVPN Service Module (WebVPN)
- Cisco VPN 5000 Concentrators
- Cisco PIX Firewalls
- Cisco Adaptive Security Appliance (ASA)
- Any Cisco device that runs Cisco's Internetwork Operating System (IOS)
- Any Cisco device that runs Cisco's Catalyst Operating System (CatOS)

No other Cisco products are currently known to contain these vulnerabilities.

Details

Hypertext Transfer Protocol (HTTP) is a set of rules for exchanging files (text, graphic images, sound, video, and other multimedia files) on the World Wide Web. HTTP is an application protocol for which the default TCP port is 80. Due to this vulnerability, a malicious user may send crafted HTTP packets which may result in a reload of the affected device and/or user connections being dropped.

The affected products are only vulnerable if they have the HTTP service enabled. By default, HTTP is enabled on VPN 3000 devices, however it may be manually disabled. Affected devices are not vulnerable to transit traffic, only traffic that is destined to them may exploit this vulnerability.

To check if the HTTP service is enabled, please do the following:

1. Check the configuration on the device to verify the status of the HTTP service.
2. Try to connect to the device using a standard web browser that supports using a URL similar to `http://ip_address_of_device/`.

This vulnerability is documented in the Cisco Bug Toolkit as Bug ID [CSCsb77324](#) ([registered](#) customers only) and [CSCsd26340](#) ([registered](#) customers only) .

Vulnerable versions of Cisco VPN 3000 do not manage certain TCP connections aggressively, which may leave the concentrator vulnerable to a denial of service attack.

- **CSCsb77324** – A malicious user may be able to send a small series of crafted HTTP packets to a concentrator which will cause the device to halt and drop user connections. The power must then be reset on the device to recover.
- **CSCsd26340** – The concentrator does not manage TCP connections to port 80 aggressively enough, leading to a scenario where memory and other resources are consumed with open connections. In specific scenarios, the concentrator will stall and drop user connections. The device must then be restarted via console access or by resetting power on the device. Alternatively, the device will recover automatically within about 20 minutes, however during this time the device is unavailable except via console access.

Impact

Successful exploitation of these vulnerabilities may cause the device to halt and drop user connections.

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.

Vulnerability	Affected Major Release	First Fixed Release
HTTP DoS Attack (CSCsb77324)	4.0.X or earlier	Not Vulnerable
	4.1.X	Not Vulnerable
	4.7.2.	4.7.2.B
TCP Attack (CSCsd26340)	4.0.X or earlier	Not Vulnerable
	4.1.X	4.1.7.L
	4.7.X	4.7.2.F

Cisco VPN 3000 series users can upgrade to version 4.1.7.L or 4.7.2.F or later software to resolve both vulnerabilities.

Cisco VPN 3000 software is available for download at <http://www.cisco.com/cgi-bin/tablebuild.pl/vpn3000-3des>.

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.

Workarounds

This section provides workarounds for this vulnerability.

Disable HTTP

Disabling HTTP will effectively mitigate this vulnerability.

With HTTP disabled, the concentrator can be configured to use HTTPS (HyperText Transfer Protocol Secure) for both concentrator management and WebVPN connectivity if WebVPN connectivity is configured on the concentrator.

To implement this workaround, first enable HTTPS, then disable HTTP.

If WebVPN is used, it is important to also disable any HTTP proxies that may be configured (HTTPS is always enabled for WebVPN if WebVPN is enabled).

For details on how to enable HTTPS management of the concentrator, please reference:

http://www.cisco.com/en/US/docs/security/vpn3000/vpn3000_47/configuration/guide/tunnel.html#wp1309312

For details on how to disable HTTP management of the concentrator, please reference:

http://www.cisco.com/en/US/docs/security/vpn3000/vpn3000_47/configuration/guide/mgtproto.html#wp999607

For details on how to disable WebVPN HTTP proxies, please reference:

http://www.cisco.com/en/US/docs/security/vpn3000/vpn3000_47/configuration/guide/tunnel.html#wp1400335

Infrastructure ACLs

HTTP to the VPN3000 could be blocked as part of an Infrastructure ACL on screening routers, switches and firewalls controlling all access to the trusted network. Infrastructure ACLs are considered a network security best practice and should be considered as a long-term addition to good network security, as well as a workaround for this specific vulnerability. The white paper entitled "Protecting Your Core: Infrastructure Protection Access Control Lists" presents guidelines and recommended deployment techniques:

http://www.cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a00801a1a55.shtml

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 not aware of any malicious use of the vulnerability described in this advisory.

These issues were reported to Cisco by Eldon Sprickerhoff from Esentire and discussed at the Shmooscon security conference on January 14th, 2006.

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-20060126-vpn.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-teams@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.

Revision History

Revision 2.1	14 August 2007	Fixed link.
Revision 2.0	26 April 2006	Updated to include DDTS
Revision 1.1	01 February 2006	CSCsd26340. – Corrected impact of successful exploitation of this vulnerability – device halts instead of reloading. – Fixed typo in name of security conference where this vulnerability was discussed.
Revision 1.0	26 January 2006	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>.

[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: Aug 14, 2007

Document ID: 68869
