

# [NEWS] Cisco VPN 3000 Concentrators DoS

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-02/msg00007.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxx)>
  - *Date:* 2 Feb 2006 10:43:37 +0200
- 

The following security advisory is sent to the securiteam mailing list, and can be found at the S  
- - promotion

The SecuriTeam alerts list - Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

- - - - -

Cisco VPN 3000 Concentrators DoS

---

## 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 a crafted HTTP (Hypertext Transfer Protocol) packet to the concentrators which may cause the device to reload and drop user connections from the Cisco VPN 3000 series.

## DETAILS

### Vulnerable Systems:

- \* Cisco VPN 3000 series concentrators version 4.7.0 and above
- \* Cisco VPN 3005 series concentrators version 4.7.0 and above
- \* Cisco VPN 3015 series concentrators version 4.7.0 and above
- \* Cisco VPN 3020 series concentrators version 4.7.0 and above
- \* Cisco VPN 3030 series concentrators version 4.7.0 and above
- \* Cisco VPN 3060 series concentrators version 4.7.0 and above
- \* Cisco VPN 3080 series concentrators version 4.7.0 and above
- \* Cisco VPN 3000 series concentrators version 4.7.2 and prior
- \* Cisco VPN 3005 series concentrators version 4.7.2 and prior
- \* Cisco VPN 3015 series concentrators version 4.7.2 and prior
- \* Cisco VPN 3020 series concentrators version 4.7.2 and prior
- \* Cisco VPN 3030 series concentrators version 4.7.2 and prior
- \* Cisco VPN 3060 series concentrators version 4.7.2 and prior
- \* Cisco VPN 3080 series concentrators version 4.7.2 and prior
- \* Cisco VPN 3000 series concentrators version 4.7REL.
- \* Cisco VPN 3005 series concentrators version 4.7REL.
- \* Cisco VPN 3015 series concentrators version 4.7REL.
- \* Cisco VPN 3020 series concentrators version 4.7REL.
- \* Cisco VPN 3030 series concentrators version 4.7REL.
- \* Cisco VPN 3060 series concentrators version 4.7REL.

## [NEWS] Cisco VPN 3000 Concentrators DoS

\* Cisco VPN 3080 series concentrators version 4.7REL.

### Immune Systems:

- \* Cisco VPN 3002 Hardware Client
- \* Cisco IPsec VPN Services Module (VPNSM)
- \* 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)
- \* Cisco VPN 3000 series concentrators version 4.6.x and prior
- \* Cisco VPN 3000 series concentrators version 4.7.2.B and above

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/>.

Successful exploitation of this vulnerability may result in a reload of the affected device and user connections being dropped.

Repeated exploitation of this vulnerability could result in a sustained Denial of Service.

### Workarounds:

#### 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 proxys 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/products/hw/vpndevc/ps2284/products\\_configuration\\_guide\\_chapter09186a](http://www.cisco.com/en/US/products/hw/vpndevc/ps2284/products_configuration_guide_chapter09186a)

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

[http://www.cisco.com/en/US/products/hw/vpndevc/ps2284/products\\_configuration\\_guide\\_chapter09186a](http://www.cisco.com/en/US/products/hw/vpndevc/ps2284/products_configuration_guide_chapter09186a)

## [NEWS] Cisco VPN 3000 Concentrators DoS

For details on how to disable WebVPN HTTP proxies please see:

[http://www.cisco.com/en/US/products/hw/vpndevc/ps2284/products\\_configuration\\_guide\\_chapter09186a](http://www.cisco.com/en/US/products/hw/vpndevc/ps2284/products_configuration_guide_chapter09186a)

### Infrastructure ACLs:

HTTP to the VPN3000 could be blocked as part of a 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\\_paper09186a00801ala55.shtml](http://www.cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a00801ala55.shtml)> Prot

### Vendor Status:

Cisco VPN 3000 series users can upgrade to version 4.7.2.B or later software to resolve this vulnerability. Cisco VPN 3000 software is available for download at

<http://www.cisco.com/cgi-bin/tablebuild.pl/vpn3000-3des>  
<http://www.cisco.com/cgi-bin/tablebuild.pl/vpn3000-3des>

### ADDITIONAL INFORMATION

The information has been provided by <mailto:psirt@xxxxxxxx> Cisco Product Security.

The original article can be found at:

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

=====

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@](mailto:list-unsubscribe@)

In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@xxxxxxxx](mailto:list-subscribe@xxxxxxxx)

=====  
=====

### 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,