

# Cisco VPN 3000 Concentrator Vulnerable to Crafted SSL Attack

Advisory ID: [cisco-sa-20050330-vpn3k](#)

<http://www.cisco.com/warp/public/707/cisco-sa-20050330-vpn3k.shtml>

## Revision 1.1

For Public Release 2005 April 06 1600 UTC (GMT)

---

Please provide your [feedback](#) on this document.

---

## Contents

- [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 a crafted attack via SSL (Secure Sockets Layer) to the concentrators which may cause the device to reload, and/or drop user connections.

Repeated exploitation will create a sustained DoS (denial of service).

Workarounds are available to mitigate this vulnerability.

Cisco has made free software available to address this vulnerability for all affected customers.

This vulnerability is documented in the Cisco Bug Toolkit as Bug ID [CSCeg11424](#) ( [registered](#) customers only)

This advisory is available at <http://www.cisco.com/warp/public/707/cisco-sa-20050330-vpn3k.shtml>

[\[Expand all sections\]](#)   [\[Collapse all sections\]](#)

## ☐ **Affected Products**

This section provides details on affected products.

### ☐ **Vulnerable Products**

Cisco VPN 3000 series concentrators running software 4.1.7.A and earlier are affected by this vulnerability.

This series includes models 3005, 3015, 3020, 3030, 3060, 3080 and the Cisco VPN 3002 Hardware Client.

### ☐ **Products Confirmed Not Vulnerable**

The following products are confirmed not vulnerable:

- Cisco IPsec VPN Services Module (VPNSM)
- Cisco VPN 5000 Concentrators
- Cisco PIX Firewalls
- 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 this vulnerability.

[Top of the section](#)   [Close Section](#)

## ☐ **Details**

Secure Sockets Layer (SSL) is a protocol used to encrypt the data transferred over a TCP session. SSL in Cisco products is mainly used by the HyperText Transfer Protocol Secure (HTTPS) web service for which the default TCP port is 443. Due to this vulnerability, a malicious user may send crafted HTTPS packets which may result in a reload of the affected device or and/or user connections being dropped.

The affected products are only vulnerable if they have the HTTPS service enabled and the access to the service is not limited to trusted hosts or network management workstations. By default, HTTPS is not enabled on VPN 3000 devices, and must be manually enabled. Affected devices are not vulnerable to transit traffic, only traffic that is destined to them may exploit this vulnerability.

To check if the HTTPS service is enabled, one can do the following:

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

No authentication is required to exploit this vulnerability.

This vulnerability is documented in the Cisco Bug Toolkit as Bug ID [CSCeg11424](#) ( [registered](#) customers only)

[Top of the section](#)   [Close Section](#)

## ☐ **Impact**

Successful exploitation of this vulnerability may result in a reload of the affected device or and/or user connections being dropped. Repeated exploitation of this vulnerability could result in a sustained Denial of Service.

[Top of the section](#)   [Close Section](#)

## ☐ **Software Versions and Fixes**

Cisco VPN 3000 series users can upgrade to version 4.1.7.B or later software to resolve this vulnerability.

When considering software upgrades, please also consult <http://www.cisco.com/warp/public/707/advisory.html> 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") for assistance.

[Top of the section](#)   [Close Section](#)

## ☐ **Workarounds**

### **Disable HTTPS**

Disabling HTTPS will effectively mitigate this vulnerability, provided the concentrator is used only for IPSEC, PPTP or L2TP over IPsec VPN connections. If the concentrator is configured for WebVPN connectivity, disabling HTTPS will also render WebVPN inoperable.

For details on how to disable HTTPS, please reference [www.cisco.com/en/US/docs/security/vpn3000/vpn3000\\_47/configuration/guide/tunnel.html#wp1309633](http://www.cisco.com/en/US/docs/security/vpn3000/vpn3000_47/configuration/guide/tunnel.html#wp1309633).

### **Transit ACLs**

SSL to the VPN3000 could be blocked as part of a Transit ACL on screening routers, switches and firewalls controlling all access to the trusted network. Transit 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 "Transit Access Control Lists: Filtering at Your Edge" presents guidelines and recommended deployment techniques for transit ACLs:

<http://www.cisco.com/warp/public/707/tacl.html>.

The effectiveness of any workaround 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 is the most appropriate for use in the intended network before it is deployed.

[Top of the section](#)   [Close Section](#)

## ☐ **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.

[Top of the section](#)   [Close Section](#)

## ☐ **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>.

[Top of the section](#)   [Close Section](#)

## ☐ **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.

[Top of the section](#)   [Close Section](#)

## ☐ **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](mailto: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.

[Top of the section](#)   [Close Section](#)

## ☐ **Exploitation and Public Announcements**

The Cisco PSIRT is not aware of any public announcements or malicious use of the vulnerability described in this advisory.

This vulnerability was discovered during internal Cisco security review.

[Top of the section](#)   [Close Section](#)

## ☐ **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.

[Top of the section](#)   [Close Section](#)

## ☐ **Distribution**

This advisory will be posted on Cisco's worldwide website at <http://www.cisco.com/warp/public/707/cisco-sa-20050330-vpn3k.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](mailto:cust-security-announce@cisco.com)
- [first-teams@first.org](mailto:first-teams@first.org) (includes CERT/CC)
- [bugtraq@securityfocus.com](mailto:bugtraq@securityfocus.com)
- [vulnwatch@vulnwatch.org](mailto:vulnwatch@vulnwatch.org)
- [cisco@spot.colorado.edu](mailto:cisco@spot.colorado.edu)
- [cisco-nsp@puck.nether.net](mailto:cisco-nsp@puck.nether.net)
- [full-disclosure@lists.grok.org.uk](mailto:full-disclosure@lists.grok.org.uk)
- [comp.dcom.sys.cisco@newsgate.cisco.com](mailto: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.

[Top of the section](#)   [Close Section](#)

## ☐ **Revision History**

Revision 1.1	2007-August-14	Fixed Link.
Revision 1.0	2005-April-06	Initial 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](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>.

Help us help you.

**Please rate this document.**

- Excellent
- Good
- Average
- Fair
- Poor

**This document solved my problem.**

- Yes
- No
- Just browsing

**Suggestions for improvement:**

(256 character limit)

