

[Solutions](#) [Products](#) [Ordering](#) [Support](#) [Partners](#) [Training](#) [Corporate](#)

Security Notices

# Cisco Security Notice: Cisco IPSec VPN Implementation Group Name Enumeration Vulnerability

## Revision 1.4

**Last Updated** 2007 August 14 1600 UTC (GMT)

**For Public Release** 2005 June 24 1300 UTC (GMT)

---

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

---

## Contents

[Summary](#)

[Details](#)

[Affected Products](#)

[Software Versions and Fixes](#)

[Obtaining Fixed Software](#)

[Workarounds and Mitigation](#)

[Acknowledgment](#)

[Status of This Notice: FINAL](#)


[Revision History](#)

[Cisco Security Procedures](#)

[Related Information](#)

---

## Summary

This Cisco Security Notice is being released in response to the Cisco VPN Concentrator Group Name Enumeration Vulnerability advisory published on June 20, 2005 by NTA Monitor at <http://www.nta-monitor.com/news/vpn-flaws/cisco/VPN-Concentrator/index.htm> .

Cisco has made free software available to address this vulnerability.

This security notice is posted at <http://www.cisco.com/warp/public/707/cisco-sn-20050624-vpn-grpname.shtml>.

## Details

This vulnerability allows an attacker to discover which group names are configured and valid on those Cisco devices listed as affected in the [Affected Products](#) section. It only affects customers using a PSK (pre-shared key) for group authentication in a remote access VPN scenario. Site-to-site VPNs (either using a PSK or certificates), customers using remote access VPNs with certificates, or customers using the VPN 3000 Concentrator feature called 'Mutual Group Authentication' are not affected by this vulnerability.

The vulnerability resides in the way those products listed as affected respond to IKE Phase I messages in Aggressive Mode. If the group name in the IKE message was a valid group name, the affected device would reply to the IKE negotiation, while an invalid group name will not elicit a response.

Once a valid group name has been identified, the attacker can use the information contained in the reply packet sent by the affected device to mount an off-line attack and try to discover the PSK used for group authentication. If the off-line attack is successful and the PSK is recovered, the information could then be used to attempt a MiTM (Man-in-the-Middle) attack against sessions being initiated by remote VPN clients towards the affected device.

This issue is documented in the following Bug IDs ([registered](#) customers only):

- [CSCeg00323](#), [CSCsb38075](#), and [CSCsf25725](#) - for the Cisco VPN 3000 Series Concentrators
- [CSCei29901](#) - for the Cisco PIX 500 Series Security Appliances running code version 7.x
- [CSCei51783](#) - for the Cisco ASA 5500 Series Adaptive Security Appliances running code version 7.x
- [CSCsb26495](#) and [CSCsb33172](#) - for Cisco IOS<sup>®</sup> software

## Affected Products

### Vulnerable Products

The following products are affected by this vulnerability:

- Cisco VPN 3000 Series Concentrators (models 3005, 3015, 3020, 3030, 3060, and 3080) running any software version earlier than v4.1.7G or v4.7.2
- Cisco PIX 500 Series Security Appliances running code version 7.x earlier than 7.0(4)
- Cisco ASA 5500 Series Adaptive Security Appliances running code version 7.x earlier than 7.0(4)
- Cisco IOS software

No other Cisco products are currently known to be affected by this vulnerability.

## Software Versions and Fixes

When considering software upgrades, please also consult [http://www.cisco.com/en/US/products/products\\_security\\_advisories\\_listing.html](http://www.cisco.com/en/US/products/products_security_advisories_listing.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.

Each row of the products table (below) lists the earliest possible release that contains the fix (the "First Fixed Release") and the anticipated date of availability. A product running a release that is earlier than the listed release (less than the First Fixed Release) is known to be vulnerable. The product should be upgraded at least to the indicated release or a later release (greater than or equal to the First Fixed Release label.)

<b>Product</b>	<b>Affected version</b>	<b>First Fixed Release</b>
Cisco VPN 3000 Concentrator family	all versions earlier than 4.1.7G	4.1.7G - available now on CCO (includes fixes for CSCeg00323 and CSCsb38075)
Cisco VPN 3000 Concentrator family	4.7.Rel	4.7.2 - available now on CCO (includes fixes for CSCeg00323 and CSCsb38075)
Cisco PIX 500 Series Security Appliances	7.x earlier than 7.0(4)	7.0(4) - available now on CCO
Cisco ASA 5500 Series Adaptive Security Appliances	7.x earlier than 7.0(4)	7.0(4) - available now on CCO
Cisco IOS Software	Please consult following table.	Please consult following table.

There is no fixed software for CSCsf25725 at the time of this writing. This Security Notice will be updated with such information once fixed software becomes available. Customers concerned about this issue should implement the workarounds listed for CSCsf25725 as required.

<b>Major Release</b>	<b>Availability of Repaired Releases</b>	
<b>Affected 12.0-Based Release</b>	<b>Rebuild</b>	<b>Maintenance</b>
12.0T	Vulnerable; migrate to 12.2(33) or later	
12.0XA	Vulnerable; migrate to 12.2(33) or later	
12.0XC	Vulnerable; migrate to 12.2(33) or later	

12.0XE	Vulnerable; migrate to 12.1(27)E or later	
12.0XG	Vulnerable; migrate to 12.2(33) or later	
12.0XH	Vulnerable; migrate to 12.2(33) or later	
12.0XI	Vulnerable; migrate to 12.2(33) or later	
12.0XJ	Vulnerable; migrate to 12.2(33) or later	
12.0XK	Vulnerable; migrate to 12.2(33) or later	
12.0XL	Vulnerable; migrate to 12.2(33) or later	
12.0XN	Vulnerable; migrate to 12.2(33) or later	
12.0XQ	Vulnerable; migrate to 12.2(33) or later	
12.0XR	Vulnerable; migrate to 12.2(33) or later	
12.0XV	Vulnerable; migrate to 12.2(33) or later	
<b>Affected 12.1-Based Release</b>	<b>Rebuild</b>	<b>Maintenance</b>
12.1	Vulnerable; migrate to 12.2(33) or later	
12.1AX	Vulnerable; migrate to 12.2(25)EY or later	
12.1AY	Vulnerable; migrate to 12.1(22)EA8 or later	
12.1AZ	Vulnerable; migrate to 12.1(22)EA8 or later	
12.1E	12.1(26)E6	12.1(27)E
12.1EA	12.1(22)EA8	
12.1EB	Vulnerable; contact TAC	
12.1EC	Vulnerable; migrate to 12.3(13a) BC2 or later	
12.1EW	Vulnerable; migrate to 12.2(18)EW or later	
	Vulnerable; migrate to 12.1(27)E or	

12.1EX	later
12.1EY	Vulnerable; migrate to 12.1(27)E or later
12.1GA	Vulnerable; migrate to 12.2(33) or later
12.1GB	Vulnerable; migrate to 12.2(33) or later
12.1T	Vulnerable; migrate to 12.2(33) or later
12.1XC	Vulnerable; migrate to 12.2(33) or later
12.1XF	Vulnerable; migrate to 12.3(16) or later
12.1XG	Vulnerable; migrate to 12.3(16) or later
12.1XH	Vulnerable; migrate to 12.2(33) or later
12.1XI	Vulnerable; migrate to 12.2(33) or later
12.1XJ	Vulnerable; migrate to 12.3(16) or later
12.1XM	Vulnerable; migrate to 12.3(16) or later
12.1XP	Vulnerable; migrate to 12.3(16) or later
12.1XQ	Vulnerable; migrate to 12.3(16) or later
12.1XT	Vulnerable; migrate to 12.3(16) or later
12.1YB	Vulnerable; migrate to 12.3(16) or later
12.1YC	Vulnerable; migrate to 12.3(16) or later
12.1YD	Vulnerable; migrate to 12.3(16) or later
12.1YE	Vulnerable; migrate to 12.3(16) or later
12.1YF	Vulnerable; migrate to 12.3(16) or later
12.1YI	Vulnerable; migrate to 12.3(16) or later

	later	
<b>Affected 12.2-Based Release Rebuild</b>	<b>Rebuild</b>	<b>Maintenance</b>
12.2		12.2(33)
12.2B	Vulnerable; migrate to 12.3(11)T9 or later	
12.2BC	Vulnerable; migrate to 12.3(13a) BC2 or later	
12.2BW	Vulnerable; migrate to 12.3(16) or later	
12.2BY	Vulnerable; migrate to 12.3(11)T9 or later	
12.2BZ	Vulnerable; migrate to 12.3(7)XI8 or later	
12.2CX	Vulnerable; migrate to 12.3(13a) BC2 or later	
12.2CY	Vulnerable; migrate to 12.3(13a) BC2 or later	
12.2CZ	Vulnerable; contact TAC	
12.2DD	Vulnerable; migrate to 12.3(11)T9 or later	
12.2S	12.2(14)S3	
	12.2(18)S13	
	12.2(20)S4	
	12.2(22)S2	
	12.2(25)S2	
		12.2(30)S
12.2SBA	12.2(27)SBA5	
12.2SBB	12.2(27)SBB2	
12.2SU	Vulnerable; migrate to 12.3(11)T9 or later	
12.2SW	12.2(25)SW6	
12.2SX	Vulnerable; migrate to 12.2(18) SXD7 or later	
12.2SXA	Vulnerable; migrate to 12.2(18) SXD7 or later	
12.2SXB	Vulnerable; migrate to 12.2(18) SXD7 or later	

12.2SXD	12.2(18)SXD7	
12.2SXE	12.2(18)SXE5	
12.2SXF	12.2(18)SXF2	
12.2SY	Vulnerable; migrate to 12.2(18)SXD7 or later	
12.2T	Vulnerable; migrate to 12.3(16) or later	
12.2XA	Vulnerable; migrate to 12.3(16) or later	
12.2XB	Vulnerable; migrate to 12.3(16) or later	
12.2XD	Vulnerable; migrate to 12.3(16) or later	
12.2XE	Vulnerable; migrate to 12.3(16) or later	
12.2XG	Vulnerable; migrate to 12.3(16) or later	
12.2XH	Vulnerable; migrate to 12.3(16) or later	
12.2XI	Vulnerable; migrate to 12.3(16) or later	
12.2XJ	Vulnerable; migrate to 12.3(16) or later	
12.2XK	Vulnerable; migrate to 12.3(16) or later	
12.2XL	Vulnerable; migrate to 12.3(16) or later	
12.2XM	Vulnerable; migrate to 12.3(16) or later	
12.2XN	Vulnerable; migrate to 12.3(16) or later	
12.2XQ	Vulnerable; migrate to 12.3(16) or later	
12.2XS	Vulnerable; migrate to 12.3(16) or later	
12.2XT	Vulnerable; migrate to 12.3(16) or later	
12.2XU	Vulnerable; migrate to 12.3(16) or later	
	Vulnerable; migrate to 12.3(16) or later	

12.2XV	later
12.2XW	Vulnerable; migrate to 12.3(16) or later
12.2YA	Vulnerable; migrate to 12.3(16) or later
12.2YB	Vulnerable; migrate to 12.3(16) or later
12.2YC	Vulnerable; migrate to 12.3(16) or later
12.2YD	Vulnerable; migrate to 12.3(11)T9 or later
12.2YE	Vulnerable; migrate to 12.2(30)S or later
12.2YF	Vulnerable; migrate to 12.3(16) or later
12.2YJ	Vulnerable; migrate to 12.3(16) or later
12.2YL	Vulnerable; migrate to 12.3(11)T9 or later
12.2YM	Vulnerable; migrate to 12.3(11)T9 or later
12.2YN	Vulnerable; migrate to 12.3(11)T9 or later
12.2YQ	Vulnerable; migrate to 12.3(11)T9 or later
12.2YR	Vulnerable; migrate to 12.3(11)T9 or later
12.2YU	Vulnerable; migrate to 12.3(11)T9 or later
12.2YV	Vulnerable; migrate to 12.3(11)T9 or later
12.2YW	Vulnerable; migrate to 12.3(11)T9 or later
12.2YX	Vulnerable; migrate to 12.3(11)T9 or later
12.2YY	Vulnerable; migrate to 12.3(11)T9 or later
12.2YZ	Vulnerable; migrate to 12.2(30)S or later
12.2ZA	Vulnerable; migrate to 12.2(18)

	SXD7 or later	
12.2ZB	Vulnerable; migrate to 12.3(11)T9 or later	
12.2ZD	Vulnerable; contact TAC	
12.2ZE	Vulnerable; migrate to 12.3(16) or later	
12.2ZF	Vulnerable; migrate to 12.3(11)T9 or later	
12.2ZG	Vulnerable; contact TAC	
12.2ZH	Vulnerable; contact TAC	
12.2ZJ	Vulnerable; migrate to 12.3(11)T9 or later	
12.2ZL	Vulnerable; contact TAC	
12.2ZN	Vulnerable; migrate to 12.3(11)T9 or later	
<b>Affected 12.3-Based Release</b>	<b>Rebuild</b>	<b>Maintenance</b>
12.3	12.3(10f)	
		12.3(16)
12.3B	Vulnerable; migrate to 12.3(11)T9 or later	
12.3BC	12.3(13a)BC2	
12.3T	12.3(4)T13; available 30-Oct-2006	
	12.3(11)T9	
		12.3(14)T6
12.3TPC	Vulnerable; contact TAC	
12.3XA	Vulnerable; contact TAC	
12.3XB	Vulnerable; migrate to 12.3(11)T9 or later	
12.3XC	Vulnerable; contact TAC	
12.3XD	Vulnerable; migrate to 12.3(11)T9 or later	
12.3XE	Vulnerable; contact TAC	
12.3XF	Vulnerable; migrate to 12.3(11)T9 or later	
12.3XG	Vulnerable; contact TAC	

12.3XH	Vulnerable; migrate to 12.3(11)T9 or later	
12.3XI	12.3(7)XI8	
12.3XJ	Vulnerable; migrate to 12.3(14)YX or later	
12.3XK	Vulnerable; migrate to 12.3(14)T6 or later	
12.3XQ	Vulnerable; migrate to 12.4(5) or later	
12.3XR	Vulnerable; contact TAC	
12.3XS	Vulnerable; migrate to 12.4(5) or later	
12.3XU	Vulnerable; migrate to 12.4(2)T3 or later	
12.3XW	Vulnerable; migrate to 12.3(14)YX or later	
12.3XX	Vulnerable; migrate to 12.4(5) or later	
12.3YA	Vulnerable; migrate to 12.4(5) or later	
12.3YD	Vulnerable; migrate to 12.4(2)T3 or later	
12.3YF	Vulnerable; migrate to 12.3(14)YX or later	
12.3YG	Vulnerable; migrate to 12.4(2)T3 or later	
12.3YH	Vulnerable; migrate to 12.4(2)T3 or later	
12.3YI	Vulnerable; migrate to 12.4(2)T3 or later	
12.3YK	Vulnerable; migrate to 12.4(4)T or later	
12.3YM	12.3(14)YM4	
12.3YQ	12.3(14)YQ5	
12.3YS	Vulnerable; migrate to 12.4(4)T or later	
12.3YT	Vulnerable; migrate to 12.4(4)T or later	
12.3YU	Vulnerable; migrate to 12.4(4)T or later	

12.3YX		12.3(14)YX
<b>Affected 12.4-Based Release</b>	<b>Rebuild</b>	<b>Maintenance</b>
12.4	12.4(1b)	
	12.4(3a)	
		12.4(5)
12.4T	12.4(2)T3	
		12.4(4)T
12.4XA	Vulnerable; migrate to 12.4(6)T or later	
12.4XB	12.4(2)XB1	

## Obtaining Fixed Software

### 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 assistance with the upgrade, which should be free of charge.

### 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)

Please 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.

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

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.

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>.

## Workarounds and Mitigation

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.

There is no specific workaround to prevent the discovery of valid group names on affected software versions using a PSK as authentication mechanism in remote access scenarios.

Customers concerned about secondary exploitation (off-line PSK recovery, MiTM attacks) can apply the following mitigation strategies:

- Use strong passwords as PSK for group authentication and change them frequently. This is the most effective way to mitigate dictionary attacks.
- For the VPN 3000 Series Concentrators only: deploy a feature called 'Mutual Group Authentication'. Additional information about this feature can be found in the [Related Information](#) section of this document.

## Acknowledgment

Cisco would like to thank NTA-Monitor for their cooperation on this issue.

## Status of This Notice: FINAL

THIS SECURITY NOTICE IS PROVIDED ON AN "AS IS" BASIS AND DOES NOT IMPLY ANY KIND OF GUARANTEE OR WARRANTY, INCLUDING THE WARRANTY OF MERCHANTABILITY. YOUR USE OF THE INFORMATION ON THE NOTICE OR MATERIALS LINKED FROM THE NOTICE IS AT YOUR OWN RISK. CISCO RESERVES THE RIGHT TO CHANGE OR UPDATE THIS NOTICE AT ANY TIME.

A stand-alone copy or Paraphrase of the text of this Security Notice that omits the distribution URL in the following section is an uncontrolled copy, and may lack important information or contain factual errors.

## Revision History

Revision 1.4	2007- August-14	Fixed link.
-----------------	--------------------	-------------


Revision 1.3	2006-November-09	Added Bug IDs and fixed software table for Cisco IOS software.
Revision 1.2	2006-September-01	Added new information for VPN3000 appliances.
Revision 1.1	2006-April-18	Added information about PIX and ASA devices. Modified first fixed release information for VPN3000 devices.
Revision 1.0	2005-June-24	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](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>.

## Related Information

- NTA-Monitor advisory - <http://www.nta-monitor.com/news/vpn-flaws/cisco/VPN-Concentrator/index.htm> 
- Mutual Group Authentication - VPN Client 4.0.5 release notes - [http://www.cisco.com/en/US/products/sw/secursw/ps2308/prod\\_release\\_note09186a0080379b](http://www.cisco.com/en/US/products/sw/secursw/ps2308/prod_release_note09186a0080379b)
- Mutual Group Authentication - VPN Client 4.6 Admin guide - [http://www.cisco.com/en/US/docs/security/vpn\\_client/cisco\\_vpn\\_client/vpn\\_client46/administ](http://www.cisco.com/en/US/docs/security/vpn_client/cisco_vpn_client/vpn_client46/administ)

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)

<a href="#">Home</a>	<a href="#">How to Buy</a>	<a href="#">Login</a>	<a href="#">Profile</a>	<a href="#">Feedback</a>	<a href="#">Site Map</a>	<a href="#">Help</a>
----------------------	----------------------------	-----------------------	-------------------------	--------------------------	--------------------------	----------------------

All contents are Copyright © 2006-2007 Cisco Systems, Inc. All rights reserved. [Important Notices](#) and [Privacy Statement](#).