



CVE-2005-3774

Published on: 11/22/2005 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:23 PM UTC

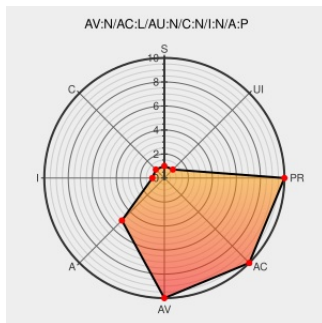
CVE-2005-3774

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Pix](#) from [Cisco](#) contain the following vulnerability:

Cisco PIX 6.3 and 7.0 allows remote attackers to cause a denial of service (blocked new connections) via spoofed TCP packets that cause the PIX to create embryonic connections that that would not produce a valid connection with the end system, including (1) SYN packets with invalid checksums, which do not result in a RST; or, from an external interface, (2) one byte of "meaningless data," or (3) a TTL that is one less than needed to reach the internal destination.

CVE-2005-3774 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **5 - MEDIUM**

Access Vector

Access Complexity

Authentication

NETWORK

LOW

NONE

Confidentiality Impact

Integrity Impact

Availability Impact

NONE

NONE

PARTIAL

CVE References

Description

Tags

Link

IBM X-Force Exchange

[exchange.xforce.ibmcloud.com](https://exchange.xforce.ibmcloud.com/text/html)
[text/html](#)

[XF cisco-pix-ttl-dos\(25079\)](#)

Cisco Security Notice: Response to Cisco PIX embryonic state machine TTL(n-1) DoS and Cisco PIX embryonic state machine 1b data DoS [Cisco PIX 500 Series Security Appliances] - Cisco Systems

[www.cisco.com](https://www.cisco.com/text/html)
[text/html](#)

CONFIRM
www.cisco.com/en/US/products/hw/vpndevc/ps2030/products_security_notice09186a

[Full-disclosure] Cisco PIX TCP Connection Prevention	Vendor Advisory web.archive.org text/html Inactive Link Not Archived	FULLDISC 20051122 Cisco PIX TCP Connection Prevention
SecurityTracker.com Archives - Cisco PIX Firewall Lets Remote Users Block TCP Connections By Spoofing Packets with Invalid Checksums	securitytracker.com text/html	SECTRAK 1015256
No Description Provided	www.osvdb.org Inactive Link Not Archived	OSVDB 24140
SecurityFocus	www.securityfocus.com text/html	BUGTRAQ 20060307 Cisco PIX embryonic state machine TTL(n-1) DoS
Cisco - Networking, Cloud, and Cybersecurity Solutions	www.cisco.com text/html	CISCO 20051128 Response to Cisco PIX TCP Connection Prevention
US-CERT Vulnerability Note VU#853540	US Government Resource www.kb.cert.org text/html	CERT-VN VU#853540
SecurityFocus	www.securityfocus.com text/html	BUGTRAQ 20051122 Cisco PIX TCP Connection Prevention
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	www.vupen.com text/html	VUPEN ADV-2005-2546
[Full-disclosure] Cisco PIX TCP Connection Prevention	web.archive.org text/html Inactive Link Not Archived	FULLDISC 20051122 Cisco PIX TCP Connection Prevention
Secunia - Advisories - Cisco PIX Spoofed TCP SYN Packets Denial of Service	web.archive.org text/html	SECUNIA 17670
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF cisco-pix-tcp-data-field-dos(25077)
Cisco PIX TCP SYN Packet Denial Of Service Vulnerability	cve.report (archive) text/html	BID 15525
SecurityFocus	www.securityfocus.com text/html	BUGTRAQ 20060307 Cisco PIX embryonic state machine 1b data DoS
SecurityFocus	www.securityfocus.com text/html	BUGTRAQ 20060307 RE: Cisco PIX embryonic state machine 1b data DoS

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware  	Cisco	Pix	6.3	All	All	All
Hardware  	Cisco	Pix	7.0	All	All	All
Hardware  	Cisco	Pix	6.3	All	All	All
Hardware  	Cisco	Pix	7.0	All	All	All
cpe:2.3:h:cisco:pix:6.3:*:*:*:*:*:						
cpe:2.3:h:cisco:pix:7.0:*:*:*:*:*:						
cpe:2.3:h:cisco:pix:6.3:*:*:*:*:*:						
cpe:2.3:h:cisco:pix:7.0:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

© [CVE.report](#) 2023  |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)