

[NEWS] Cisco PIX Multiple Vulnerabilities

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-11/0065.html>

From: support@securiteam.com

Date: 11/21/02

From: support@securiteam.com

To: list@securiteam.com

Date: 21 Nov 2002 11:27:49 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

Beyond Security would like to welcome Tiscali World Online to our service provider team.

For more info on their service offering IP-Secure, please visit http://www.worldonline.co.za/services/work_ip.asp

Cisco PIX Multiple Vulnerabilities

SUMMARY

The Cisco PIX Firewall provides robust, enterprise-class security services including stateful inspection firewalling, standards-based IP Security (IPsec) Virtual Private Networking (VPN), intrusion protection and much more in cost-effective, easy to deploy solutions.

Two vulnerabilities have been resolved for the PIX firewall for which fixes are available. These vulnerabilities are documented as Cisco bug ID CSCdv83490 and CSCdx35823. There are no workarounds available to mitigate the effects of these vulnerabilities.

DETAILS

Affected Products:

All PIX Firewall units running the vulnerable releases and using the specific features are affected by these vulnerabilities.

No other Cisco products are currently known to be affected by these vulnerabilities.

DDTs – Description:

CSCdv83490 – While processing initial contact notify messages the PIX does

Securiteam: [NEWS] Cisco PIX Multiple Vulnerabilities

not delete duplicate Internet Security Authentication Key Management Protocol Security Associations (ISAKMP SAs) with the peer.

Affected Release:

- * 6.0.3 and earlier
- * 6.1.3 and earlier

DDTs – Description:

CSCdx35823 – Buffer overflow while doing HTTP traffic authentication using Terminal Access Controller Access Control System Plus (TACACS+) or Remote Authentication Dial-In User Service (RADIUS).

Affected Release:

- * 5.2.8 and earlier
- * 6.0.3 and earlier
- * 6.1.3 and earlier
- * 6.2.1 and earlier

To determine your software revision, type show version at the command line prompt.

Details:

CSCdv83490

When a user establishes a VPN session upon successful peer and user authentication, the PIX creates an ISAKMP SA associating the user and his IP address.

If an attacker is now able to block the logged-in user's connection and establish a connection to the PIX using the same IP address as that of the user, he will be able to establish a VPN session with the PIX, using only peer authentication, provided he already has access to the peer authentication key also known as the group pre-shared key (PSK) or group password key.

CSCdx35823

A user starting a connection via FTP, Telnet, or over the World Wide Web (HTTP) is prompted for their user name and password. If the user name and password are verified by the designated TACACS+ or RADIUS authentication server, the PIX Firewall unit will allow further traffic between the authentication server and the connection to interact independently through the PIX Firewall unit's "cut-through proxy" feature.

The PIX may crash and reload due to a buffer overflow vulnerability while processing HTTP traffic requests for authentication using TACACS+ or RADIUS.

The Internetworking Terms and Acronyms online guide can be found at <http://www.cisco.com/univercd/cc/td/doc/cisintwk/ita/index.htm> <http://www.cisco.com/univercd/cc/td/doc/cisintwk/ita/index.htm>. The Cisco Systems Terms and Acronyms online guide can be found at <http://www.cisco.com/univercd/cc/td/doc/cisintwk/ita/cisco12.htm>

Securiteam: [NEWS] Cisco PIX Multiple Vulnerabilities

<http://www.cisco.com/univercd/cc/td/doc/cisintwk/ita/cisco12.htm>.

These vulnerabilities are documented in the Bug Toolkit as Bug IDs CSCdv83490 and CSCdx35823, and can be viewed after 2002 November 21 at 1600 UTC. To access this tool, you must be a registered user and you must be logged in.

Impact:

DDTs – Description:

CSCdv83490 – While processing initial contact notify messages the PIX does not delete duplicate ISAKMP SA's with the peer.

Impact:

This vulnerability can be exploited to initiate a Man–In–The–Middle attack for VPN sessions to the PIX.

DDTs – Description

CSCdx35823 – Buffer overflow while doing HTTP traffic authentication using TACACS+ or RADIUS.

Impact:

This vulnerability can be exploited to initiate a Denial–of–Service attack.

Software Versions and Fixes:

DDTs – Description:

CSCdv83490 – While processing initial contact notify messages the PIX does not delete duplicate ISAKMP SAs with the peer.

Fixed Releases:

- * 6.0.4 and later
- * 6.1.4 and later
- * 6.2.1 and later

DDTs – Description:

CSCdx35823 – Buffer overflow while doing HTTP traffic authentication using TACACS+ or RADIUS.

Fixed Releases:

- * 5.2.9 and later
- * 6.0.4 and later
- * 6.1.4 and later
- * 6.2.2 and later

The procedure to upgrade to the fixed software version is detailed at

<http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_sw/index.htm>
http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_sw/index.htm.

Obtaining Fixed Software:

Cisco is offering free software upgrades to address these vulnerabilities for all affected customers. Customers may only install and expect support for the feature sets they have purchased.

Securiteam: [NEWS] Cisco PIX Multiple Vulnerabilities

Customers with service contracts should contact their regular update channels to obtain the free software upgrade identified via this advisory.

To access the software download URL

<<http://www.cisco.com/cgi-bin/tablebuild.pl/pix>>

<http://www.cisco.com/cgi-bin/tablebuild.pl/pix>, you must be a registered user and you must be logged in. For most customers with service contracts, this means that upgrades should be obtained through the Software Center on Cisco's worldwide website at

<<http://www.cisco.com/cgi-bin/tablebuild.pl/pix>>

<http://www.cisco.com/cgi-bin/tablebuild.pl/pix>.

Customers whose Cisco products are provided or maintained through a 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 obtaining the free software upgrade(s).

Customers who purchased directly 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 obtain fixed software by contacting the Cisco Technical Assistance Center (TAC) using the contact information listed below. In these cases, customers are entitled to obtain an upgrade to a later version of the same release or as indicated by the applicable corrected software version in the Software Versions and Fixes section (noted above).

Cisco 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

See <<http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>>

<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.

Please have your product serial number available and give the URL of this advisory as evidence of your entitlement to a free upgrade.

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

Workarounds:

There are no workarounds for these vulnerabilities. The Cisco PSIRT recommends that affected users upgrade to a fixed software version of code.

ADDITIONAL INFORMATION

The original advisory can be viewed by going to:

<<http://www.cisco.com/warp/public/707/pix-multiple-vuln-pub.shtml>>

Securiteam: [NEWS] Cisco PIX Multiple Vulnerabilities

<http://www.cisco.com/warp/public/707/pix-multiple-vuln-pub.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@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

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, consequential, loss of business profits or special damages.