

Table of Contents

<u>Cisco Security Notice: Response to BugTraq – PIX Denial of Service</u>	1
<u>Document ID: 59820</u>	1
<u>Revision 1.0</u>	1
<u>Last Updated 2001 April 06</u>	1
<u>Please provide your feedback on this document</u>	1
<u>Summary</u>	1
<u>Details</u>	1
<u>Cisco Security Procedures</u>	4

Cisco Security Notice: Response to BugTraq – PIX Denial of Service

Document ID: 59820

Revision 1.0

Last Updated 2001 April 06

Please provide your feedback on this document.

[Summary](#)
[Details](#)
[Cisco Security Procedures](#)

Summary

This document is provided to simplify access to Cisco responses to possible product security vulnerability issues posted in public forums for Cisco customers. This does not imply that Cisco perceives each of these issues as an actual product security vulnerability. This notice is provided on an "as is" basis and does not imply any kind of guarantee or warranty. Your use of the information on the page or materials linked from this page are at your own risk. Cisco reserves the right to change or update this page without notice at any time.

Details

Original Report: <http://www.securityfocus.com/archive/1/174577> . Cisco responded with the following, which is also archived at <http://www.securityfocus.com/archive/1/174698> .

```
To: BugTraq
Subject: Re: PIX Firewall 5.1 DoS Vulnerability
Date: Apr 6 2001 8:52PM
Author: Lisa Napier <lnapier@cisco.com>
Message-ID: <4.3.2.7.2.20010406160412.03c0abc0@171.70.24.186>
In-Reply-To: <20010406070650.6755.qmail@securityfocus.com>
```

Hi Claudiu,

The Cisco Technical Assistance Center is working on this case currently. We do not typically comment on cases that are still actively being worked. If you feel that progress is not being made on the case, please alert the case owner, or ask to speak with a manager.

The engineers working this case have been working to reproduce the problem, engineering is also working on the problem in conjunction with the customer support engineer. The crash info you have provided has not been helpful due to another defect, CSCdp66094, which causes the 5.1 series of code to continuously reload once the defect has been triggered with non-informative crash info.

The crash does not occur in the later versions of code, and the 5.1 series

of code is not recommended for customers due to the following announcement.
http://www.cisco.com/warp/customer/cc/pd/fw/sqfw500/prodlit/1303_pp.htm

At this point we are still investigating the possible options for a fix.

Thank you,

Lisa Napier
Product Security Incident Response Team
Cisco Systems

At 12:06 AM 01/04/06, Claudiu Calomfirescu wrote:
>06.04.2001
>Datanet Systems
>Claudiu Calomfirescu
>claudiu datanets ro
>
>
>PIX Firewall 5.1 DoS Vulnerability
>
>
>Description:
>-----
>An attacker from inside or outside interfaces of a
>PIX Firewall 515 or 520, 5.1.4 version running aaa
>authentication against a TACACS+ Server could
>cause the PIX to crash and reload by overwhelming
>it with authentication requests.
>
>
>Products affected:
>-----
>Vulnerable Product: PIX Firewall 515, 520
>Vulnerable OS: 5.1.4 - General Deployment
>Release
>Non Vulnerable OS: 5.3.1 - General Deployment
>Release
>
>
>Vendor response:
>-----
>The vendor (Cisco Systems) was noticed on 14 March
>(TAC case number B215177) and till now they only
>asked about the environment in which was found,
>without really trying to reproduce. They received
>the exploit program, PIX configuration, detailed
>description about whats happened, stack trace from
>the crash, logs.
>
>
>How was found:
>-----
>1. A user from inside without aaa permission to go
>out, play a game (Jewels) from zapspot.com. - he
>does not know a thing about what is happening in
>the background.
>
>2. At a certain time, the game try to connects to
>the address api.zapspot.com on port 80 from port
>2000.
>
>3. The pix start an authentication process, but
>the game is not a browser and the user dont see a

```

>thing, after that, the game try to connects to the
>address api.zapsport.com on port 80 from port 2001,
>2002, 2003 and so on very very quickly (hundreds
>per seconds)
>
>4. The pix has too many authentication in progress
>and crash.
>
>
>Discussion:
>-----
>
>To reproduce the problem do the following:
>
>1. Configure the PIX Firewall version 5.1.4 for
>aaa authentication against a TACACS+ server:
>
>aaa-server TACACS+ protocol tacacs+
>aaa-server RADIUS protocol radius
>aaa-server grup protocol tacacs+
>aaa-server grup (inside) host 10.10.10.20 cheia
>timeout 5
>aaa authentication include http outbound 0.0.0.0
>0.0.0.0 0.0.0.0 0.0.0.0 grup
>aaa authorization include http outbound 0.0.0.0
>0.0.0.0 0.0.0.0 0.0.0.0 grup
>aaa accounting include http outbound 0.0.0.0
>0.0.0.0 0.0.0.0 0.0.0.0 grup
>
>2. From an inside host generate http request with
>sweep source port directed to a global address on
>port 80.
>
>In our case we generate a http request from port
>2000, the pix start an authentication process:
>
>109001: Auth start for user '???' from
>10.10.10.1/2000 to 216.46.233.11/80
>
>after that we generate a http request from port
>2001,
>
>109001: Auth start for user '???' from
>10.10.10.1/2001 to 216.46.233.11/80
>
>and so on. After 426 requests (this number is not
>always the same) generated in 3 seconds the PIX
>give the message:
>
>Panic: uauth1 - open: no more channels
>(tcp/UNPROXY/1/0)!
>
>and crashed in:
>
>Thread Name: uauth1 (Old pc 0x80070b4f ebp
>0x810c56dc)
>
>and reloads.
>
>Very simple and nice.
>
>
>
>Version 5.3.1 is more stable, till now I could not

```

```
>get it down, I could consume all resources, but it
>didnt crash:
>
>701001: alloc_user() out of Tcp_user objects
>109010: Auth from 10.10.10.1/2440 to
>216.46.233.11/80 failed (too many pending auths)
>on interface inside
>
>We had available only PIX Firewall models 515 and
>520.
>
>
>-----
>-----
>Claudiu Calomfirescu                               Datanet
>Systems SRL
>IT Security Consultant                             Zarii 14,
>sector 5
>mobile: + 40 94 20 33 55                           Bucharest,
>Romania
>email: claudiu datanets ro                          tel: + 40
>1 22 33 755
>http://www.datanets.ro                             fax: + 40
>1 22 33 747
>-----
>-----
```

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. This includes instructions for press inquiries regarding Cisco security notices. All Cisco security advisories are available at <http://www.cisco.com/go/psirt>.

All contents are Copyright © 1992–2005 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Updated: Jul 14, 2005

Document ID: 59820
