

# Cisco Security Advisory: Cisco Secure PIX Firewall SMTP Filtering Vulnerability

Document ID: 15235

Advisory ID: cisco-sa-20010926-pix-firewall-smtp-filter

<http://www.cisco.com/warp/public/707/cisco-sa-20010926-pix-firewall-smtp-filter>

## Version 1.1

Last Updated 2001 September 28 0800 UTC (GMT)

For Public Release 2001 September 26 1500 UTC (GM)

---

Please provide your feedback on this document.

---

[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 Secure PIX firewall feature "mailguard" which limits SMTP commands to a specified minimum set of commands can be bypassed.

This vulnerability can be exploited to bypass SMTP command filtering.

This vulnerability has been assigned Cisco bug ID CSCdu47003.

The complete notice will be available at  
<http://www.cisco.com/warp/public/707/cisco-sa-20010926-pix-firewall-smtp-filter.shtml>.

## Affected Products

This section provides details on affected products.

## Vulnerable Products

All users of Cisco Secure PIX Firewalls with software versions 6.0(1), 5.2(5) and 5.2(4) that provide access to SMTP Mail services are at risk. Please see the table below for affected versions.

## Products Confirmed Not Vulnerable

The IOS Firewall feature set is not affected by the above defect.

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

## Details

The behavior is a failure of the command **fixup protocol smtp [portnum]**, which is enabled by default on the Cisco Secure PIX Firewall. The impact and description of this defect is similar to a defect outlined in a previous security advisory, <http://www.cisco.com/warp/public/707/PIXfirewallSMTPfilter-pub.shtml>, however, this instance of mail filtering bypass was re-introduced by the defect CSCds90792.

If you do not have protected Mail hosts with the accompanying configuration (configuration example below) you are not vulnerable to the attack.

To exploit this vulnerability, attackers must be able to make connections to an SMTP mail server protected by the PIX Firewall. If your Cisco Secure PIX Firewall has configuration lines similar to the following:

```
fixup protocol smtp 25
```

and either

```
conduit permit tcp host 192.168.0.1 eq 25 any
```

or

```
conduit permit tcp 192.168.0.1 255.255.255.0 eq 25 any
```

or

```
access-list 100 permit tcp any host 192.168.0.1 eq 25
```

```
access-group 100 in interface outside
```

The expected filtering of the Mailguard feature can be circumvented by an attacker.

## Impact

If the mail server itself is not properly secured, an attacker may be able to collect information about existing e-mail accounts and aliases, or may be able to execute arbitrary code on the mail server. In order to exploit this vulnerability, an attacker would need to also exploit the mailserver that is currently protected by the PIX. If that server is already well configured, and has the latest security patches and fixes from the SMTP vendor, that will minimize the potential for exploitation of this vulnerability.

Please note that Cisco strongly recommends that security on all servers, workstations and network infrastructure gear is maintained as part of Standard Operating Procedures. Internet Firewalls do not protect against risk factors internal to a Firewalled network such as social engineering, rogue internal users or additional external access points to the internal network (i.e. modem pools or network fax machines) and as such should not be viewed as the only security measure necessary to ensure network integrity.

## Software Versions and Fixes

The following table of affected software versions and fixes details ALL affected versions, including engineering special builds that are rarely provided to customers. The "Affected Products" section above mentions only the versions that have been officially released. For example, in version 4.4(7) the defect was introduced in 4.4(7.202) and fixed in 4.4(7.204). As there was no officially released version between those two engineering builds, it is unlikely that any customer would have the affected version, however, this is documented as resolved in the Release Notes for version 4.4(8).

Version Affected	Interim Release Fix will carry forward into all later versions	Fixed Regular Release; available now Fix will carry forward into all later versions
4.4(7.202)	4.4(7.204)	4.4(8)
5.1(4.206)	5.1(4.209)	5.1(5)
5.2(3.210)	5.2(5.207)	5.2(6)
5.3(1.200)	5.3(1.206)	5.3(2)
6.0(1)	6.0(1.101)	6.1(1)

## Workarounds

There is not a direct workaround for this vulnerability. The potential for exploitation can be lessened by ensuring that mail servers are secured without relying on the PIX functionality.

## 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.

## 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 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.

## 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.

## Exploitation and Public Announcements

This vulnerability was discovered internally by Cisco, during expanded regression testing. This vulnerability has been discussed on public forums previously. This vulnerability has not been discussed recently, and has not been discussed with reference to the current versions of the PIX software.

## 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.

## Distribution

This advisory will be posted on Cisco's worldwide website at <http://www.cisco.com/warp/public/707/cisco-sa-20010926-pix-firewall-smtp-filter.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)
- [bugtraq@securityfocus.com](mailto:bugtraq@securityfocus.com)
- [first-teams@first.org](mailto:first-teams@first.org) (includes CERT/CC)
- [cisco@spot.colorado.edu](mailto:cisco@spot.colorado.edu)
- [comp.dcom.sys.cisco](mailto:comp.dcom.sys.cisco)
- [firewalls@lists.gnac.com](mailto:firewalls@lists.gnac.com)
- Various internal Cisco mailing lists

Future updates of this advisory, if any, will be placed on Cisco's Worldwide Web server, 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.

## Revision History

Revision 1.1	2001-September-28	In the section "Software Versions and Fixes" added an explanation of affected software versions.
Revision 1.0	2001-September-26	For 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>.

---

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

---

Updated: Sep 26, 2001

Document ID: 15235

---