

Cisco Security Advisory: Cisco IOS Firewall Authentication Proxy for FTP and Telnet Sessions Buffer Overflow

Document ID: 66269

Advisory ID: cisco-sa-20050907-auth_proxy

http://www.cisco.com/warp/public/707/cisco-sa-20050907-auth_proxy.shtml

Revision 1.3

Last Updated 2005 October 12 2005 1800 UTC (GMT)

For Public Release 2005 September 07 1600 UTC (GMT)

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 IOS Firewall Authentication Proxy for FTP and/or Telnet Sessions feature in specific versions of Cisco IOS software is vulnerable to a remotely-exploitable buffer overflow condition.

Devices that do not support, or are not configured for Firewall Authentication Proxy for FTP and/or Telnet Services are not affected.

Devices configured with only Authentication Proxy for HTTP and/or HTTPS are not affected.

Only devices running certain versions of Cisco IOS[®] are affected.

Cisco has made free software available to address this vulnerability. There are workarounds available to mitigate the effects of the vulnerability.

This advisory will be posted at

http://www.cisco.com/warp/public/707/cisco-sa-20050907-auth_proxy.shtml.

Affected Products

This section provides details on affected products.

Vulnerable Products

Devices that are running the following release trains of Cisco IOS are affected if Firewall Authentication Proxy for FTP and/or Telnet Sessions is configured and applied to an active interface.

- 12.2SG, 12.2SEC, 12.2SXF, 12.2SH, 12.2ZF and 12.2ZL based trains
- 12.3 based trains
- 12.3T based trains
- 12.4 based trains
- 12.4T based trains

To determine the software running on a Cisco product, log in to the device and issue the **show version** command to display the system banner. Cisco IOS software will identify itself as "Internetwork Operating System Software" or simply "IOS." On the next line of output, the image name will be displayed between parentheses, followed by "Version" and the Cisco IOS release name. Other Cisco devices will not have the show version command, or will give different output.

The following example identifies a Cisco 7200 router running Cisco IOS release 12.3(10a) with an installed image name of C7200-JK8O3S-M.

```
Router# show version
Cisco Internetwork Operating System Software
IOS (tm) 7200 Software (C7200-JK8O3S-M), Version 12.3(10a), RELEASE SOFTWARE (fc2)
Copyright (c) 1986-2004 by cisco Systems, Inc.
```

Additional information about Cisco IOS release naming can be found at <http://www.cisco.com/warp/public/620/1.html>.

Refer to the [Details](#) section for more information about affected and unaffected configurations.

Products Confirmed Not Vulnerable

These products are not vulnerable:

- Products that are not running Cisco IOS are not affected.
- Products that are running Cisco IOS versions 12.2 and earlier (including 12.0S) are not affected. (excluding those listed).
- Products that are running Cisco IOS are not affected unless they are configured for Firewall Authentication Proxy for FTP and/or Telnet Sessions.
- Products that are running Cisco IOS XR are not affected.

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

Details

The Cisco IOS Firewall Authentication Proxy feature allows network administrators to apply specific security policies on a per-user basis. With the Firewall Authentication Proxy for FTP and/or Telnet Sessions feature, users can log into the network services via FTP and/or Telnet, and their specific access profiles are automatically retrieved and applied from a Remote Authentication Dial In User Service (RADIUS), or

Terminal Access Controller Access Control System Plus (TACACS+) authentication server.

Cisco IOS Software is vulnerable to a Denial of Service (DoS) and potentially an arbitrary code execution attack when processing the user authentication credentials from an Authentication Proxy Telnet/FTP session. To exploit this vulnerability an attacker must first complete a TCP connection to the IOS device running affected software and receive an auth-proxy authentication prompt.

This vulnerability is documented in the Cisco Bug Toolkit as Bug ID [CSCsa54608](#) ([registered](#) customers only) .

To determine if your device is running the Firewall Authentication Proxy for FTP and/or Telnet Sessions feature, log into the device and issue the **show ip auth-proxy configuration** command to display the configuration of Firewall Authentication Proxy services. The following example identifies Firewall Authentication Proxy services running for Telnet and FTP under the proxy rule name **proxy_example**.

```
Router# show ip auth-proxy configuration
Authentication global cache time is 60 minutes
Authentication global absolute time is 0 minutes
Authentication Proxy Watch-list is disabled

Authentication Proxy Rule Configuration
Auth-proxy name proxy_example
ftp list not specified auth-cache-time 60 minutes
telnet list not specified auth-cache-time 60 minutes
```

The following will be seen if Firewall Authentication Proxy services are not enabled but supported in your IOS version:

```
Router# show ip auth-proxy configuration
Authentication global cache time is 60 minutes
Authentication global absolute time is 0 minutes
Authentication Proxy Watch-list is disabled

Router#
```

The following will be seen if running a version of IOS that does not support Firewall Authentication Proxy services:

```
Router# show ip auth-proxy configuration
      ^
% Invalid input detected at '^' marker.

Router#
```

A router that has Firewall Authentication Proxy services assigned to an interface will have **ip auth-proxy list name** command under an interface in the **show running-config** output.

The following example identifies Firewall Authentication Proxy services running under the proxy rule name "proxy_example" applied to the interface Ethernet 2/1:

```
Router# show ip auth-proxy configuration
Authentication global cache time is 60 minutes
Authentication global absolute time is 0 minutes
Authentication Proxy Watch-list is disabled

Authentication Proxy Rule Configuration
Auth-proxy name proxy_example
      ftp not specified auth-cache-time 60 minutes
      telnet specified auth-cache-time 60 minutes

Router# show running-config
```

```

.
.
!
interface Ethernet2/1
 ip address 10.1.1.1 255.255.255.0
 ip auth-proxy proxy_example
!
.
.

```

Additional information about Cisco IOS Firewall Authentication Proxy services refer to: http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t5/iosfw2/iosfw2_1.htm.

Additional information about Cisco IOS Firewall Authentication Proxy for FTP and/or Telnet Sessions refer to: http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123_1/ftp_tel.htm

Impact

Successful exploitation of the vulnerability on Cisco IOS may result in a reload of the device or execution of arbitrary code. Repeated exploitation could result in a sustained DoS attack or execution of arbitrary code on Cisco IOS devices.

Software Versions and Fixes

When considering software upgrades, please also consult 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 Cisco IOS software table (below) describes a release train and the platforms or products for which it is intended. If a given release train is vulnerable, then the earliest possible releases that contain the fix (the "First Fixed Release") and the anticipated date of availability for each are listed in the "Rebuild" and "Maintenance" columns. A device running a release in the given train that is earlier than the release in a specific column (less than the First Fixed Release) is known to be vulnerable. The release should be upgraded at least to the indicated release or a later version (greater than or equal to the First Fixed Release label).

For further information on the terms "Rebuild" and "Maintenance", please consult the following URL: <http://www.cisco.com/warp/public/620/1.html>.

Major Release	Availability of Repaired Releases	
	Rebuild	Maintenance
Affected 12.2–Based Release		
12.2SG	Vulnerable; contact TAC	
12.2SEC	Vulnerable; contact TAC	
12.2SXF	Vulnerable; contact TAC	
12.2SH	Vulnerable; 12.2(13)ZH8, available 25–Oct–05	

12.2ZF	Vulnerable; migrate to 12.3T or later	
12.2ZL	Vulnerable; migrate to 12.3(4)XK4 or later for Cisco 17xx; migrate to 12.4(1) or later for Cisco 3200; migrate to 12.3(7)XR4 or later for ICS7750.	
Affected 12.3–Based Release	Rebuild	Maintenance
12.3	12.3(3h)	
	12.3(5e)	
	12.3(6e)	
	12.3(9d)	
	12.3(10d)	
	12.3(12b)	
	12.3(13a)	12.3(15)
12.3B	Vulnerable; migrate to 12.3(14)T2 or later	
12.3BC	12.3(9a)BC7; available 19–Sept–05	
12.3BW	Vulnerable; migrate to 12.3(14)T2 or later	
12.3JA		12.3(7)JA
12.3JK		12.3(2)JK
12.3T	12.3(7)T10	
	12.3(8)T9	
	12.3(11)T6	
	12.3(14)T2	
12.3XA	12.3(2)XA5; available TBD	
12.3XB	Vulnerable; migrate to 12.3(14)T2 or later	
12.3XC	12.3(2)XC3	
12.3XD	Vulnerable; migrate to 12.3(14)T2 or later	
12.3XE	12.3(2)XE4; available TBD	
12.3XF	Vulnerable; migrate to 12.3(14)T2 or later	
12.3XG	12.3(4)XG5; available TBD	
12.3XH	Vulnerable; migrate to 12.3(14)T2 or later	

12.3XI	12.3(7)XI4	
12.3XJ	Vulnerable; migrate to 12.3(11)YF2 or later	
12.3XK	12.3(4)XK4; available TBD	
12.3XL	12.3(11)XL3	
12.3XM	Vulnerable; migrate to 12.3(14)T2 or later	
12.3XQ	Vulnerable; migrate to 12.4(1) or later	
12.3XR	12.3(7)XR4	
12.3XS	Vulnerable; migrate to 12.4(1) or later	
12.3XU	Vulnerable; contact TAC	
12.3XW	Vulnerable; migrate to 12.3(11)YF2 or later	
12.3XY	Vulnerable; contact TAC	
12.3YA	Vulnerable; migrate to 12.4(1) or later for Cisco 828; migrate to 12.3(8)YG2 or later for SOHO 9x, Cisco 83x	
12.3YD	Vulnerable; migrate to 12.3(14)T2 or later	
12.3YF	12.3(11)YF2	
12.3YG	12.3(8)YG2	
12.3YI	12.3(8)YI1	
12.3YJ	Vulnerable; contact TAC	
12.3YK	12.3(11)YK1	
12.3YQ		12.3(14)YQ
12.3YS		12.3(11)YS
12.3YT		12.3(14)YT
12.3YU		12.3(14)YU
12.3YW		12.3(11)YW
Affected 12.4–Based Release	Rebuild	Maintenance
12.4		12.4(1)
12.4MR		12.4(2)MR
12.4T		12.4(2)T

Workarounds

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.

- **Disable Cisco IOS Firewall Authentication Proxy feature for Telnet/FTP sessions.**

In networks where Cisco IOS Firewall Authentication Proxy feature for Telnet/FTP sessions is not required but enabled, disabling the feature on an IOS device will eliminate exposure to this vulnerability. On a router which is configured for Cisco IOS Firewall Authentication Proxy feature for Telnet/FTP sessions, this must be done by issuing the command:

no ip auth-proxy name 'auth-proxy-name' {ftp | telnet}

- **Deploy Cisco IOS Firewall Authentication Proxy feature for HTTP/HTTPS sessions.**

Configure the device with Cisco IOS Firewall Authentication Proxy feature for HTTP and/or HTTPS sessions and allow the Telnet and FTP services within the per-user TACACS+/RADIUS profile.

Disable Authentication proxy for Telnet/FTP sessions to eliminate exposure. An example of the configuration statements for HTTP session Auth-proxy is:

```
! Configure auth-proxy for http session authentication
ip auth-proxy name http-proxy http
! Configure the router's web server to service auth-proxy authentication attempts
ip http server
! Set the HTTP server authentication method to AAA
ip http authentication aaa
```

Additional auth-proxy and web server configuration settings are available. For details see

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t5/iosfw2/iosfw2_1.htm

After successful authentication via HTTP/HTTPS, the user can initiate required FTP or Telnet sessions. The example shown below for Cisco Secure Windows (TACACS+) server profile Group setting allows FTP and Telnet as part of access-list entry **proxyacl#2=permit tcp any any**

```
priv-lvl=15
proxyacl#1=permit icmp any any
proxyacl#2=permit tcp any any
proxyacl#3=permit udp any any
```

Mitigations

Not all of the mitigation strategies listed will work for all customers. Some of the workarounds listed are dependent on which versions and feature-sets of IOS you have in your network. These mitigation strategies, may help reduce exposure to this vulnerability. To eliminate exposure to this vulnerability, customers should apply one of the workarounds listed above, or upgrade to a fixed release of Cisco IOS.

- **Access Control Lists (ACLs)**

Deploying IP access-lists can mitigate the effects of this vulnerability by allowing Firewall Authentication Proxy access only from trusted subnets. This feature must be used in conjunction with interface access-lists to ensure that IP traffic from un-trusted subnets is dropped by the router and not forwarded around the auth-proxy feature. Once the IP access-list is created, it is applied to the Authentication proxy by adding the keyword **list** followed by the IP access-list name or number. In the example below the trusted network is 169.160.160.0/24 and the auth-proxy router interface is 10.66.65.47. Example:

```
! Permit trusted network 169.160.160.0/24 to access auth-proxy
access-list 105 permit tcp 169.160.160.0 0.0.0.255 any eq telnet
!
! Deny all IP traffic that is not authenticated by auth-proxy
! Note: Management and Control traffic to the router itself would
!       need to be allowed in this access-list
access-list 106 deny ip any any
```

```

!
! Modify the telnet auth-proxy config to use access-list 105
ip auth-proxy name tel-proxy telnet inactivity-time 60 list 105
!
! Apply interface access-list 106 and auth-proxy test
interface FastEthernet1/0
ip address 10.66.65.47 255.255.255.0
ip access-group 106 in
ip auth-proxy tel-proxy

```

For further information on creating IP access lists, refer to Protecting Your Core: Infrastructure Protection Access Control Lists, at

http://www.cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a00801a1a55.shtml,

and Transit Access Control Lists: Filtering at Your Edge, at

http://www.cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a00801afc76.shtml.

• Control Plane Policing

The Control Plane Policy (CoPP) feature can be used to mitigate the effects of this vulnerability by only allowing trusted hosts to attempt connections through the auth-proxy router.

Care must be taken to ensure that legitimate management connections to the auth-proxy router itself are not dropped by the CoPP policy.

In the following example trusted management host 169.160.160.1 is allowed to establish Telnet connections to the auth-proxy router itself.

Trusted network 169.160.160.0/24 is allowed to attempt FTP and Telnet auth-proxy connections to IP networks and addresses other than the auth-proxy router itself. All other inbound FTP and Telnet connections attempts are denied.

The auth-proxy router's IP addresses are 172.16.1.1 (Internet Side), 1.1.1.1/24 and 10.66.65.47 (Internal).

Telnet/FTP server is 172.168.1.1.

```

! Do not police Telnet from trusted management host 169.160.160.1 to the auth-proxy
access-list 105 remark ** Do not police telnet from Trusted Hosts to Auth-Proxy Router
access-list 105 deny tcp host 169.160.160.1 host 172.16.1.1 eq telnet
access-list 105 deny tcp host 172.168.1.1 host 1.1.1.1 eq telnet
access-list 105 deny tcp host 172.168.1.1 host 10.66.65.47 eq telnet
!
! Police all other telnet and ftp connections to the auth-proxy router
access-list 105 remark ** Police all other telnet/ftp attempts to Auth-Proxy Router
access-list 105 permit tcp any host 172.16.1.1 eq telnet
access-list 105 permit tcp any host 1.1.1.1 eq telnet
access-list 105 permit tcp any host 10.66.65.47 eq telnet
access-list 105 permit tcp any host 172.16.1.1 eq ftp
access-list 105 permit tcp any host 1.1.1.1 eq ftp
access-list 105 permit tcp any host 10.66.65.47 eq ftp
!
! Allow telnet and ftp auth-proxy for trusted network 169.160.160.0/24
access-list 105 remark ** Allow Auth-Proxy sessions from trusted networks **
access-list 105 deny tcp 169.160.160.0 0.0.0.255 any eq telnet
access-list 105 deny tcp 169.160.160.0 0.0.0.255 any eq ftp
!
! Allow telnet and ftp auth-proxy for trusted network back to 169.160.160.0/24
access-list 105 remark ** Allow Auth-Proxy sessions to trusted networks **
access-list 105 deny tcp host 172.168.1.1 169.160.160.0 0.0.0.255
!
! Allow TACACS+ from ACS server 10.66.79.229
access-list 105 remark ** Ensure we can still communicate with TACACS+ Server **
access-list 105 deny tcp host 10.66.79.229 gt 1023 host 10.66.65.47 eq 49
access-list 105 deny tcp host 10.66.79.229 eq 49 host 10.66.65.47 gt 1023
!
! Police all TCP based management traffic from un-trusted hosts
! Note: If BGP is configured it would need to be allowed before this access-list ent
access-list 105 remark ** Drop any other TCP connections **
access-list 105 permit tcp any any

```

```

!
! Do not police any other type of traffic going to the router
access-list 105 remark ** Rest do not police **
access-list 105 deny ip any any
!
class-map match-all only-allow-trusted-hosts
match access-group 105
!
policy-map control-plane-policy
! Drop all traffic that matches the class "only-allow-trusted-hosts"
  class only-allow-trusted-hosts
    drop
!
control-plane
service-policy input control-plane-policy

```

Note: CoPP is available only in IOS release trains 12.0S, 12.2S and 12.3T. Additional information on the configuration and use of the CoPP feature can be found at the following URL:

http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/prod_white_papers_list.html

- **Transit Access Control Lists**

Additional mitigation can be added by Transit Access Control Lists that filter transit and edge traffic at network ingress points should be configured so that IP traffic is only allowed from legitimate, trusted IP addresses. For more information on tACLs, refer to:

http://www.cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a00801afc76.shtml

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 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

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>.

Exploitation and Public Announcements

Since the initial posting of this document, the Cisco PSIRT has been made aware of public announcements of the vulnerabilities described in this advisory. Cisco PSIRT is aware that the exploit for this vulnerability has been published on a public mailing list.

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-20050907-auth_proxy.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
- first-teams@first.org (includes CERT/CC)
- bugtraq@securityfocus.com
- vulnwatch@vulnwatch.org
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- full-disclosure@lists.grok.org.uk

- comp.dcom.sys.cisco@newsgate.cisco.com

Future updates of this advisory, if any, will be placed on Cisco's worldwide website, 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 1.3	2005–October–12	Updated Exploitation and Public Announcements section and all 12.2 references in Affected Products .
Revision 1.2	2005–September–26	In Software Versions and Fixes table: 12.2ZH changed to 12.2SH, added 12.2ZF.
Revision 1.1	2005–September–22	Added 12.2SG, 12.2SEC, and 12.2SXF releases to Software Version and Fixes table.
Revision 1.0	2005–September–07	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. This includes instructions for press inquiries regarding Cisco security notices. All Cisco security advisories are available at <http://www.cisco.com/go/psirt>.

[Contacts & Feedback](#) | [Help](#) | [Site Map](#) © 2007 – 2008 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Oct 12, 2005

Document ID: 66269
