

Cisco Applied Mitigation Bulletin: Identifying and Mitigating Exploitation of Multiple Vulnerabilities in the IOS FTP Server

<http://www.cisco.com/warp/public/707/cisco-amb-20070509-iosftp.shtml>

Revision 1.1

For Public Release 2007 May 09 1600 UTC (GMT)

Please provide your [feedback](#) on this document.

Contents

[Cisco Response](#)

[Device-Specific Mitigation and Identification](#)

[Cisco IOS Routers and Switches](#)

[Cisco IOS NetFlow](#)

[Cisco ASA, PIX, and FWSM Firewalls](#)

[Cisco Intrusion Prevention System](#)

[Cisco Security Monitoring, Analysis, and Response System](#)

[Additional Information](#)

[Revision History](#)

[Cisco Security Procedures](#)

[Related Information](#)

Cisco Response

This Applied Mitigation Bulletin is a companion document to the PSIRT Security Advisory: *Multiple Vulnerabilities in the IOS FTP Server*. It documents additional mitigation techniques that can be deployed on Cisco devices within the network.

Vulnerability Characteristics

Multiple vulnerabilities exist in the Cisco File Transfer Protocol (FTP) server. These vulnerabilities are summarized below:

- **Improper authorization checking in IOS FTP server:** This vulnerability can be exploited remotely without valid authentication and no user interaction is necessary. The attack vector used to exploit this vulnerability is through TCP port 21 (FTP) and TCP port 20 (FTP-DATA).

This vulnerability has been assigned CVE name CVE-2007-2586.

- **IOS reload when transferring files via FTP server:** This vulnerability can be exploited remotely without valid authentication and no user interaction is necessary. Successful exploitation of this vulnerability may allow arbitrary code execution or cause the affected device to crash. Repeated attempts to exploit this vulnerability could result in a sustained denial of service (DoS) condition. The vectors used to exploit this vulnerability are TCP port 21 (FTP) and TCP port 20 (FTP-DATA). This vulnerability has been assigned CVE name CVE-2007-2587

This document contains information to assist Cisco customers in mitigating attempts to exploit *Multiple Vulnerabilities in the IOS FTP Server*. Information about vulnerable, unaffected, and fixed software is available in the PSIRT Security Advisory at

<http://www.cisco.com/warp/public/707/cisco-sa-20070509-iosftp.shtml>

Mitigation Technique Overview

Cisco devices provide several countermeasures for the *Multiple Vulnerabilities in the IOS FTP Server*. Many of these protection methods should be considered general security best practices for infrastructure devices and the traffic that transits the network.

Effective means of exploit prevention can be provided by Cisco IOS using infrastructure access control lists.

Effective means of exploit prevention can be provided by Cisco ASA 5500 Series Adaptive Security Appliance, Cisco PIX 500 Series Security Appliance, and the Firewall Services Module (FWSM) for Cisco Catalyst 6500 Series switches and Cisco 7600 Series routers using the following:

- Transit Access Control Lists
- Strict FTP Application Layer Protocol Inspection

These protection mechanisms filter and drop attempts to exploit the vulnerabilities described in this document.

The Cisco Intrusion Prevention System provides visibility into and protection against attacks trying to exploit these vulnerabilities through the effective use of event-actions.

Visibility into these exploitation attempts can be provided by Cisco IOS NetFlow using flow records, and by Cisco IOS software, Cisco ASA, Cisco PIX and FWSM firewalls through syslog messages and the counter values displayed in the output from **show** commands. Visibility can also be provided through the use of the Cisco Security Monitoring, Analysis, and Response System (Cisco Security MARS) appliance through the use of queries and event reporting.

Risk Management

Organizations should follow their standard risk mitigation process to determine the potential impact of this vulnerability. Documents that may be used to aid in risk triage are available at [Risk Triage for Security Vulnerability Announcements](#) and [Risk Triage and Prototyping](#).

Device-Specific Mitigation and Identification



Caution: The effectiveness of any mitigation technique is dependent on specific customer situations such as product mix, network topology, traffic behavior, and organizational mission. As

with any configuration change, evaluate the impact of this configuration prior to applying the change.

Specific information on mitigation and identification is available for these devices:

- [Cisco IOS Routers and Switches](#)
- [Cisco IOS NetFlow](#)
- [Cisco ASA, PIX, and FWSM Firewalls](#)
- [Cisco Intrusion Prevention System](#)
- [Cisco Security Monitoring, Analysis, and Response System](#)

Cisco IOS Routers and Switches

Mitigation: Infrastructure Access Control Lists

In an effort to protect infrastructure devices and minimize the risk, impact, and effectiveness of direct infrastructure attacks, infrastructure access control lists (iACLs) should be deployed to perform policy enforcement of traffic sent to infrastructure equipment. Administrators can construct an iACL by explicitly permitting only authorized traffic sent to infrastructure devices in accordance with existing security policies and configurations. For maximum protection of infrastructure devices, iACLs deployed on Cisco IOS routers should be applied in the ingress direction to all interfaces on which an IP address has been configured.

In the following example, the address block 192.168.134.0/24 is the infrastructure address space and the host at 192.168.208.63 is considered a trusted FTP client. The iACL policy denies FTP packets on TCP ports 21 (FTP) and 20 (FTP-DATA) sent to addresses that are part of the infrastructure address space.

Care should be taken to allow required traffic for routing and administrative access prior to denying all traffic sent directly to infrastructure devices. Whenever possible, infrastructure address space should be distinct from the address spaced used for user and services segments. Using this addressing methodology will assist with the construction and deployment of iACLs.

Additional information about iACLs is available at [Protecting Your Core: Infrastructure Protection Access Control Lists](#).

```
ip access-list extended ACL-INFRASTRUCTURE

!-- When applicable include explicit permit statements for trusted
!-- sources requiring access on the vulnerable port(s)

permit tcp host 192.168.208.63 gt 1023 192.168.134.0 0.0.0.255 eq 21
!-- FTP

permit tcp host 192.168.208.63 gt 1023 192.168.134.0 0.0.0.255 eq 20
!-- FTP-Data Active

permit tcp host 192.168.208.63 gt 1023 192.168.134.0 0.0.0.255 gt 1023
!-- FTP-Data Passive
```

```

!-- The following are vulnerability-specific access control entries
!-- (ACEs) to aid identification of attacks

deny tcp any 192.168.134.0 0.0.0.255 eq 21
deny tcp any 192.168.134.0 0.0.0.255 eq 20

!-- Explicit deny ACE for traffic sent to addresses configured within
!-- the infrastructure address space

deny ip any 192.168.134.0 0.0.0.255

!-- Permit/Deny all other Layer 3 and Layer 4 traffic in accordance with
!-- existing security policies and configurations

!-- Apply iACL to interface(s) in the ingress direction.

interface GigabitEthernet0/0
ip access-group ACL-INFRASTRUCTURE in

```

Note that filtering with an interface access list will elicit the transmission of ICMP unreachable messages back to the source of the filtered traffic. This could have the undesired effect of increasing CPU utilization because the filtering device needs to generate these ICMP unreachable messages. In IOS, ICMP unreachable generation is limited to one packet every 500 milliseconds. ICMP unreachable message generation can be disabled using the **no icmp unreachable** interface configuration command. ICMP unreachable rate limiting can be changed from the default of one per 500 milliseconds using the global configuration command **ip icmp rate-limit unreachable interval-in-ms**.

Identification: Infrastructure Access Control Lists

Once the Infrastructure ACL has been applied to an interface, the **show access-lists** command can be used to identify the number of TCP port 21 (FTP) and TCP port 20 (FTP-DATA) packets that have been filtered. Filtered packets should be investigated to determine if they are attempts to exploit this vulnerability.:

```

router#show ip access-lists ACL-INFRASTRUCTURE
Extended IP access list ACL-INFRASTRUCTURE
 10 permit tcp host 192.168.208.63 gt 1023 192.168.134.0 0.0.0.255 eq ftp
 20 permit tcp host 192.168.208.63 gt 1023 192.168.134.0 0.0.0.255 eq ftp
 30 permit tcp host 192.168.208.63 gt 1023 192.168.134.0 0.0.0.255 gt 102
 40 deny tcp any 192.168.134.0 0.0.0.255 eq ftp (5 matches)
 50 deny tcp any 192.168.134.0 0.0.0.255 eq ftp-data
 60 deny ip any 192.168.134.0 0.0.0.255

```

In the preceding example, access list ACL-INFRASTRUCTURE has dropped five TCP port 21 (FTP) packets for ACE sequence-id 40.

Identification: Access List Logging

The **log** or **log-input** ACL option will cause logging of packets that match specific ACEs. The **log-input** option enables logging of the ingress interface in addition to the packet source and destination IP addresses and ports.



Caution: ACL logging can be very CPU intensive and must be used with extreme caution. The CPU impact from ACL logging is driven by two factors: process switching as a result of packets that match **log**-enabled ACEs, and log generation and transmission.

The **ip access-list logging interval *interval-in-ms*** command can limit the effects of ACL-logging-induced process switching. The **logging rate-limit *messages-per-second* except *loglevel*** command limits the impact of log generation and transmission.

Cisco IOS NetFlow

Identification: Traffic Flow Identification Using NetFlow Records

Cisco IOS NetFlow can be configured on Cisco IOS routers and switches to aid in the identification of traffic flows that may be potential attempts to exploit the vulnerability described in this document. Flows should be compared to baseline utilization of FTP traffic sent on TCP ports 21 (FTP) and 20 (FTP-DATA). The flows should also be investigated to determine whether they are sourced from untrusted hosts or networks.

```
router#show ip cache flow
IP packet size distribution (156859151 total packets):
  1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  48
  .007 .575 .054 .008 .009 .010 .005 .013 .000 .001 .004 .001 .003 .002 .00

  512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
  .001 .001 .159 .013 .118 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 4456704 bytes
  10 active, 65526 inactive, 66950922 added
  236246619 ager polls, 0 flow alloc failures
  Active flows timeout in 1 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 402056 bytes
  20 active, 16364 inactive, 8101354 added, 6478434 added to flow
  0 alloc failures, 0 force free
  1 chunk, 11 chunks added
  last clearing of statistics never

Protocol          Total      Flows      Packets Bytes  Packets Active(Sec) Idle(Se
-----          Flows      /Sec       /Flow /Pkt   /Sec     /Flow   /Flow
TCP-Telnet       11416154    2.6         1     49    3.1      0.0     1.5
TCP-FTP          14536       0.0         5     53    0.0      3.6    11.0
TCP-FTPD         1033        0.0        2176   881    0.5     37.0     1.6
TCP-WWW          206319      0.0         12    714    0.5      4.3     9.2
TCP-SMTP          12          0.0         1     47    0.0      0.0    10.5
TCP-X             731         0.0         1     40    0.0      0.0     1.4
TCP-BGP           13          0.0         1     46    0.0      0.0    10.3
TCP-NNTP          12          0.0         1     47    0.0      0.0     9.7
TCP-Frag          70401       0.0         1    688    0.0      0.0    22.7
TCP-other        49747333   11.5         2    337   29.8     0.1     1.5
UDP-DNS           1916625     0.4         1     56    0.5      0.0    15.4
UDP-NTP           1764053     0.4         1     76    0.4      0.4    15.5
UDP-TFTP           10          0.0         2     57    0.0      6.6    18.6
UDP-other        1362009     0.3         2    161    0.6      0.3    16.4
ICMP              427507      0.0         6     49    0.6     15.0    17.9
IPv6INIP          15          0.0         1   1132    0.0      0.0    15.4
GRE               23980       0.0         19    109    0.1     57.4     1.7
IP-other           2          0.0         2     20    0.0      0.1    15.7
Total:            66950745   15.5         2    310   36.5     0.2     2.7

SrcIf      SrcIPAddress  DstIf      DstIPAddress  Pr SrcP DstP  Pk
Gi0/0     192.168.208.63 Gi0/1     192.168.134.21 06 8C7F 0015
Gi0/0     192.168.208.63 Gi0/0     192.168.135.167 06 0016 0EAD
Gi0/0     192.168.208.63 Gi0/1     192.168.134.21 06 8C89 0014 2
Gi0/0     192.168.226.1  Gi0/1     192.168.202.22 11 007B 007B
Gi0/0     192.168.226.1  Gi0/1     192.168.144.3  11 007B 007B
Gi0/0     192.168.254.17 Gi0/1     192.168.150.1  01 0000 030D
```

```

Gi0/0          192.168.128.56  Gi0/1          192.168.132.44  11 0035 E0E5
Gi0/0          192.168.208.63  Gi0/1          192.168.134.21  06 8C87 C81B  1

```

To view only FTP (IP Protocol 6, port 21, hex value 0015) and FTP-DATA (IP Protocol 6, port 20, hex value 0014) flows, the command **show ip cache flow | include SrcIf| 06 .*(014|015)** may be used to display the relevant NetFlow records, as shown here:

```

router#show ip cache flow | include SrcIf| 06 .*(014|015)
SrcIf      SrcIPAddress  DstIf      DstIPAddress  Pr  SrcP  DstP  Pk
Gi0/0     192.168.208.64  Gi0/1*    192.168.1.21  06  C845  0015
Gi0/0     192.168.208.64  Gi0/1     192.168.1.21  06  C845  0015
Gi0/0     192.168.208.64  Gi0/1*    192.168.1.21  06  C844  0014  4
Gi0/0     192.168.208.64  Gi0/1     192.168.134.21  06  C844  0014  4
Gi0/1     192.168.134.21  Gi0/0*    192.168.208.64  06  0015  C841
Gi0/1     192.168.134.21  Gi0/0*    192.168.208.64  06  0015  C845
Gi0/1     192.168.134.21  Gi0/0*    192.168.208.64  06  0014  C844  8

```

Cisco ASA, PIX, and FWSM Firewalls

Mitigation: Transit Access Control Lists

In an effort to protect the network from traffic that enters the network at ingress access points which may include Internet connection points, partner and supplier connection points, or VPN connection points, Transit Access Control Lists (tACL) should be deployed to perform policy enforcement. The construction of a tACL is accomplished by explicitly permitting only authorized traffic to enter the network at ingress access points, or permitting authorized traffic to transit the network in accordance with existing security policies and configurations.

The tACL policy denies unauthorized FTP packets on TCP ports 21 (FTP) and 20 (FTP-DATA) sent to affected devices. In the following example, 192.168.134.0/24 is the network IP address space used by the affected devices and the host at 192.168.208.63 is considered a trusted source requiring access to the affected devices. Care should be taken to allow required traffic for routing and administrative access prior to denying all unauthorized traffic.

Additional information about tACLs is available at [Transit Access Control Lists: Filtering at Your Edge](#).

Note: Default basic FTP application inspection is used to open ports for FTP data connections.

```

!-- Include any explicit permit statements for trusted sources requiring acc
!-- on the vulnerable FTP port

access-list ACL-TRANSIT extended permit tcp host 192.168.208.63 gt 1023 192.

!-- The following vulnerability-specific access control entries (ACEs) can a
!-- in the identification of attacks.

access-list ACL-TRANSIT extended deny tcp any 192.168.134.0 255.255.255.0 eq
access-list ACL-TRANSIT extended deny tcp any 192.168.134.0 255.255.255.0 eq
!

!-- Permit/Deny all other Layer 3 and Layer 4 traffic in accordance with
!-- existing security policies and configurations.

```

```

!-- Explicit Deny for all other IP traffic

access-list ACL-TRANSIT extended deny ip any any

!-- Apply tACL to interface(s) in the ingress direction.

access-group ACL-TRANSIT in interface outside

```

Mitigation: Network Access Authentication

Network access authentication can be used to mitigate the improper authentication on the IOS FTP server. Network Access Authentication is a feature that intercepts traffic that transits through the firewall by matching an access control list policy. Traffic that matches the access control list is required to be authenticated before the traffic will be permitted to transit through the firewall to the destination. Network Access Authentication does not perform authentication on behalf of the requested service.

Note: A user or users that are successfully authenticated using network access authentication can exploit the vulnerable device.

This mitigation example permits access to the Cisco FTP service to trusted users authenticated via the Access Control Server at 192.168.130.66. In the following example, a connection through the Cisco ASA or Cisco PIX to the the IOS FTP server at 192.168.128.21 causes the ASA to prompt the user with a username and password that are verified against the Access Control Server (ACS) at 192.168.130.66. This is before the FTP session is allowed to reach the vulnerable device at 192.168.128.21.

```

aaa-server ACS protocol tacacs+
aaa-server ACS host 192.168.130.66
  key UseProperKey

aaa authentication match ACL-AUTHENTICATE outside ACS

access-list ACL-AUTHENTICATE extended permit tcp any host 192.168.128.21 eq

```

Note: Users need to enter the access information in the following format:

```

host#ftp 192.168.128.21
User: ACS_user@IOSFTP_user
Password: ACS_password@IOSFTP_password

```

In this example, network authentication permits any valid user in the ACS server to to reach the host at 192.168.128.21 if configured, the network authorization feature can permit a per-user ACL.

Mitigation: Application Layer Inspection

Cisco ASA and Cisco PIX

The ASA and PIX Version 7.2 and later [FTP inspection policy map for additional inspection control](#) feature permits to filtering FTP sessions with a finer granularity and can be used to identify the Cisco IOS FTP server by matching the initial server response. Additionally, the feature can reset sessions to the Cisco IOS FTP server that uses a set of defined FTP commands.

This mitigation technique starts by matching the initial FTP server response to the known Cisco IOS FTP server response. That is, this response is matched to the following string: (Note this is the initial server response, not the response to the FTP SYST command.)

```
IOS-FTP server (version 01.00) ready
```

This matching is accomplished through a regular expression. Then, FTP application inspection is used to identify FTP commands that can potentially alter the state of the router. The FTP commands in the example that cause the FTP control session to reset are: appe help, rnfr, rnto, put, stou, site, dele, mkd, rmd.

In addition, GET commands are permitted but most other FTP commands, including those that write to the IOS FTP server, will cause the connection to reset (including PUT, APPEND, MKDIR, RENAME, DELETE and RMDIR).

```
!-- The following regular expression matches the Cisco IOS FTP server initial

regex IOS-FTP "\x20IOS-FTP\x20server\x20[(\|)version\x20[. ]00[ ])\x20ready"

!-- The inspection class map identifies FTP sessions that matches both of:
!-- The Cisco IOS FTP server initial banner AND
!-- A subset of the FTP commands, not including GET

class-map type inspect ftp match-all CMAP-ALLOW-GET-ONLY-TO-IOS-FTP
  match server regex IOS-FTP
  match request-command appe help rnfr rnto put stou site dele mkd rmd

!-- The inspection policy map resets FTP sessions
!-- that match the preceding class-map

policy-map type inspect ftp PMAP-INSPECT-FTP
  class CMAP-ALLOW-GET-ONLY-TO-IOS-FTP
    reset

!-- The inspection policy is applied to the global_policy policy-map

policy-map global_policy

  class inspection_default
    inspect ftp strict PMAP-INSPECT-FTP

!-- Apply policy to traffic entering all interfaces.

service-policy global_policy global
```

Cisco FWSM

The Catalyst 6500 Firewall Services Module [strict FTP application layer inspection](#) is capable of resetting FTP sessions that use any of a defined set of commands as indicated in the **request-command deny** ftp map configuration command. In the following configuration example, FTP

sessions for the IOS device at 192.168.128.21 that attempt to use FTP commands denied in the FMAP-FTP ftp map class will be reset.

```

!-- Identify the IOS devices that which will have their FTP sessions inspect
access-list ACL-IOS-FTP line 1 extended permit tcp any host 192.168.128.21 e

!-- List the FTP commands that will NOT be permitted to the IOS devices

ftp-map FMAP-ALLOW-GET-ONLY
  request-command deny appe help rnfr rnto put stou site dele mkd rmd

!-- Create a class-map for the FTP sessions to IOS devices

class-map CMAP-IOS-FTP

!-- Match FTP traffic to the IOS devices as indicated by ACL

match access-list ACL-IOS-FTP

!-- Create the policy-map to use

policy-map global_policy

!-- FTP traffic to the IOS devices will be inspected for denied commands

class CMAP-IOS-FTP
  inspect ftp strict FMAP-ALLOW-GET-ONLY

!-- Other ftp traffic uses default application inspection.

class inspection_default
  inspect ftp

!-- Apply policy to traffic entering all interfaces.

service-policy global_policy global

```

Identification: Transit Access Control Lists

With a transit ACL, once the access list has been applied to an interface in the ingress direction, the **show access-list** command can be used to identify the number of TCP port 21 (FTP) and TCP port 20 (FTP-DATA) packets that are being filtered. Filtered packets should be investigated to determine whether they are attempts to exploit this vulnerability. Example output of the **show access-list ACL-TRANSIT** command follows:

```

firewall#show access-list ACL-TRANSIT
access-list ACL-TRANSIT; 4 elements

```

```

access-list ACL-TRANSIT line 1 extended permit tcp host 192.168.208.63 192.1
access-list ACL-TRANSIT line 2 extended deny tcp any 192.168.134.0 255.255.2
access-list ACL-TRANSIT line 3 extended deny tcp any 192.168.134.0 255.255.2
access-list ACL-TRANSIT line 4 extended deny ip any any (hitcnt=0) 0xbe3cd3c

```

In the preceding example, the access list ACL-TRANSIT has dropped **seven packets** for TCP port 21 (FTP) received from a nontrusted host or network. This tACL is applied to the interface outside in the ingress direction. In addition, syslog message 106023 can provide valuable information, which includes the source and destination IP address, the source and destination port numbers, and the protocol for the denied packet.

Identification: Firewall Access-list Syslog Messages

Firewall syslog message 106023 will be generated for packets denied by an ACE that do not have the **log** keyword present. Additional information about this syslog message is available at [Cisco Security Appliance System Log Message - 106023](#).

Information on configuring syslog for the Cisco ASA 5500 Series Adaptive Security Appliance or the Cisco PIX 500 Series Security Appliance is available at [Configuring Logging on the Cisco Security Appliance](#). Information on configuring syslog on the FWSM for Cisco Catalyst 6500 Series switches and Cisco 7600 Series routers is available at [Configuring Monitoring and Logging on the Cisco FWSM](#).

In the following examples, the **show logging | grep regex** command is used to extract syslog messages from the logging buffer on the firewall. This is performed to obtain additional information about denied packets that could indicate potential attempts to exploit the vulnerability described in this document. It is possible to use different regex patterns with the **grep** keyword to search for specific data present within the logged messages.

```

firewall#show logging | grep 106023
Apr 13 2007 01:40:21: %ASA-4-106023: Deny tcp src outside:192.168.208.63/349
Apr 13 2007 01:40:24: %ASA-4-106023: Deny tcp src outside:192.168.208.63/349

```

In the preceding example, the messages (106023) logged for the tACL *ACL-TRANSIT* show TCP port 21 (FTP) denied packets sent to the address block assigned to the network infrastructure.

Additional information about syslog messages for ASA and PIX security appliances is available at [Cisco Security Appliance System Log Messages](#). Additional information about syslog messages for the FWSM is available at [Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Logging Configuration and System Log Messages](#).

Identification: Network Access Authentication

In order to identify users currently authenticated by the firewall, use the **show uauth** command. In the following example, two users are currently authenticated and the maximum simultaneous authenticated users is 4. The currently authenticated users are *user1* and *user2*.

```

ASA#show uauth

```

	Current	Most Seen
Authenticated Users	2	4
Authen In Progress	0	1
user ' user2 ' at 192.168.208.63, authenticated (idle for 0:01:07)		
absolute timeout:	0:05:00	
inactivity timeout:	0:00:00	
user ' user1 ' at 192.168.208.63, authenticated (idle for 0:04:59)		
absolute timeout:	0:05:00	

```
inactivity timeout: 0:00:00
```

The Firewall will produce the following syslog messages when a user is successfully authenticated. The following is the syslog message produced for successful authentication for a FTP session originated by 102.168.208.64 to the FTP server at 192.168.134.21. The Cisco ACS server at 192.168.130.66 performed the credential validation for user authentication.

The authenticated user is allowed access to the 192.168.134.21 FTP server. Network Authentication does not restrict the FTP commands available to the user.

```
%ASA-6-109001: Auth start for user '???' from 192.168.208.63/35836 to 192.16
%ASA-6-113004: AAA user authentication Successful : server = 192.168.130.66
%ASA-6-113008: AAA transaction status ACCEPT : user = user1
%ASA-2-109011: Authen Session Start: user 'user1', sid 3
%ASA-6-109005: Authentication succeeded for user 'user1' from 192.168.208.63
%ASA-5-109012: Authen Session End: user 'ftp', sid 3, elapsed 301 seconds
```

In the same scenario, a failed authentication produced the following syslog messages:

```
%ASA-6-109001: Auth start for user '???' from 192.168.208.63/57315 to 192.16
%ASA-6-113005: AAA user authentication Rejected : reason = Unspecified : ser
%ASA-6-109006: Authentication failed for user 'user1' from 192.168.208.63/57
%ASA-6-113005: AAA user authentication Rejected : reason = Unspecified : ser
```

Identification: Application Layer Inspection

Cisco ASA and Cisco PIX

The Cisco ASA 5500 Series Adaptive Security Appliance permits a FTP inspection class map. In the following example, 14 FTP sessions were reset because they attempted to use FTP commands in the CMAP-ALLOW-GET-ONLY-TO-IOS-FTP inspection class map and the FTP server matched the regular expression named IOS-FTP.

```
ASA#show service-policy inspect ftp table

Global policy:
Service-policy: global_policy
Class-map: inspection_default
Inspect: ftp strict PMAP-INSPECT-FTP, packet 471, drop 0, reset-drop 1
Class-map: CMAP-ALLOW-GET-ONLY-TO-IOS-FTP
Number of filters 2, action: reset
Filter id: 2, subid/is_regex: 0x0/0, value_type: VALUE_GENERIC
value: 4085(0xff5), value_high: 0(0x0)
mask_match: ANY, mask_value: 0x0, negate: 0
Filter id: 3, subid/is_regex: 0x0/0, value_type: VALUE_REGEX
value: 20(0x14)/IOS-FTP, value_high: 20(0x14)
mask_match: NONE, mask_value: 0x0, negate: 0
```

Syslog message 302014 indicates a FTP session that has been terminated by application inspection:

```
%ASA-6-302014: Teardown TCP connection 636005 for outside:10.89.16.92/4298 t
```

Cisco FWSM

In the following example, two FTP sessions were reset because they attempted to use FTP commands denied in the FMAP-FTP ftp class map. The traffic is matched by an ACL in the CMAP-IO-FTP class map.

```
FWSM#show service-policy
```

```
Global policy:
Service-policy: global_policy
Class-map: CMAP-IOS-FTP
  Inspect: ftp strict FMAP-ALLOW-GET-ONLY, packet 26, drop 0, reset-drop
Class-map: inspection_default
  Inspect: dns maximum-length 512, packet 0, drop 0, reset-drop 0
  Inspect: h323 h225, packet 0, drop 0, reset-drop 0
  Inspect: h323 ras, packet 0, drop 0, reset-drop 0
  Inspect: netbios, packet 0, drop 0, reset-drop 0
  Inspect: rsh, packet 0, drop 0, reset-drop 0
  Inspect: skinny, packet 0, drop 0, reset-drop 0
  Inspect: sqlnet, packet 0, drop 0, reset-drop 0
  Inspect: sunrpc, packet 0, drop 0, reset-drop 0
  Inspect: tftp, packet 0, drop 0, reset-drop 0
  Inspect: sip, packet 0, drop 0, reset-drop 0
  Inspect: xdmcp, packet 0, drop 0, reset-drop 0
  Inspect: ftp, packet 0, drop 0, reset-drop 0
```

The 303002 syslog message is produced by the FWSM when FTP inspection is active. It indicates a file was retrieved (GET) or stored (PUT) in the FTP server. In both cases the file retrieved/stored is **filename.ext**.

```
Apr 30 2007 00:57:43: %FWSM-6-303002: 192.168.150.70 Retrieved 192.168.134.
Apr 30 2007 01:41:59: %FWSM-6-303002: 192.168.150.70 Stored 192.168.134.21:
```

When strict FTP application inspection is used by the administrator, syslog message 303003 is produced when a denied FTP command causes the session to be reset, for example:

```
%FWSM-6-303003: FTP put command denied - failed strict inspection, terminati
%FWSM-6-303003: FTP rmd command denied - failed strict inspection, terminati
```

Cisco Intrusion Prevention System

Identification: IPS Signature Event Store

The Cisco Intrusion Prevention System (IPS) appliances and services modules can be used to provide threat detection and prevention against attempts to exploit the Multiple Vulnerabilities in the IOS FTP Server advisory described in this document. Starting with signature update S285 for sensors running Cisco IPS version 6.x or 5.x, connections to the Cisco IOS FTP server can be detected by signature **5860/0** (Signature Name: **IOS FTPd Successful Login**). Signature 5860/0 is enabled by default and triggers a Low severity event. Signature 5860/0 is triggered by multiple packets sent using TCP port 21. Signature 5860/0 is a meta signature, its components are signatures 5860/1 and 5846/0 which are all required to be triggered in order for the meta signature to trigger. Each of the individual meta-component subsignature therefore have no defined event action and thus are each considered an Informational severity event.

The following **Low** severity event was triggered on a Cisco IPS sensor deployed in promiscuous mode.

```
sensor6x#show events alert | include 5860
evIdsAlert: eventId=1166767918236277023 severity=low vendor=Cisco
originator:
  hostId: sensor6x
  appName: sensorApp
  appInstanceId: 27487
time: 2007/04/27 17:07:39 2007/04/27 12:07:39 CDT
```

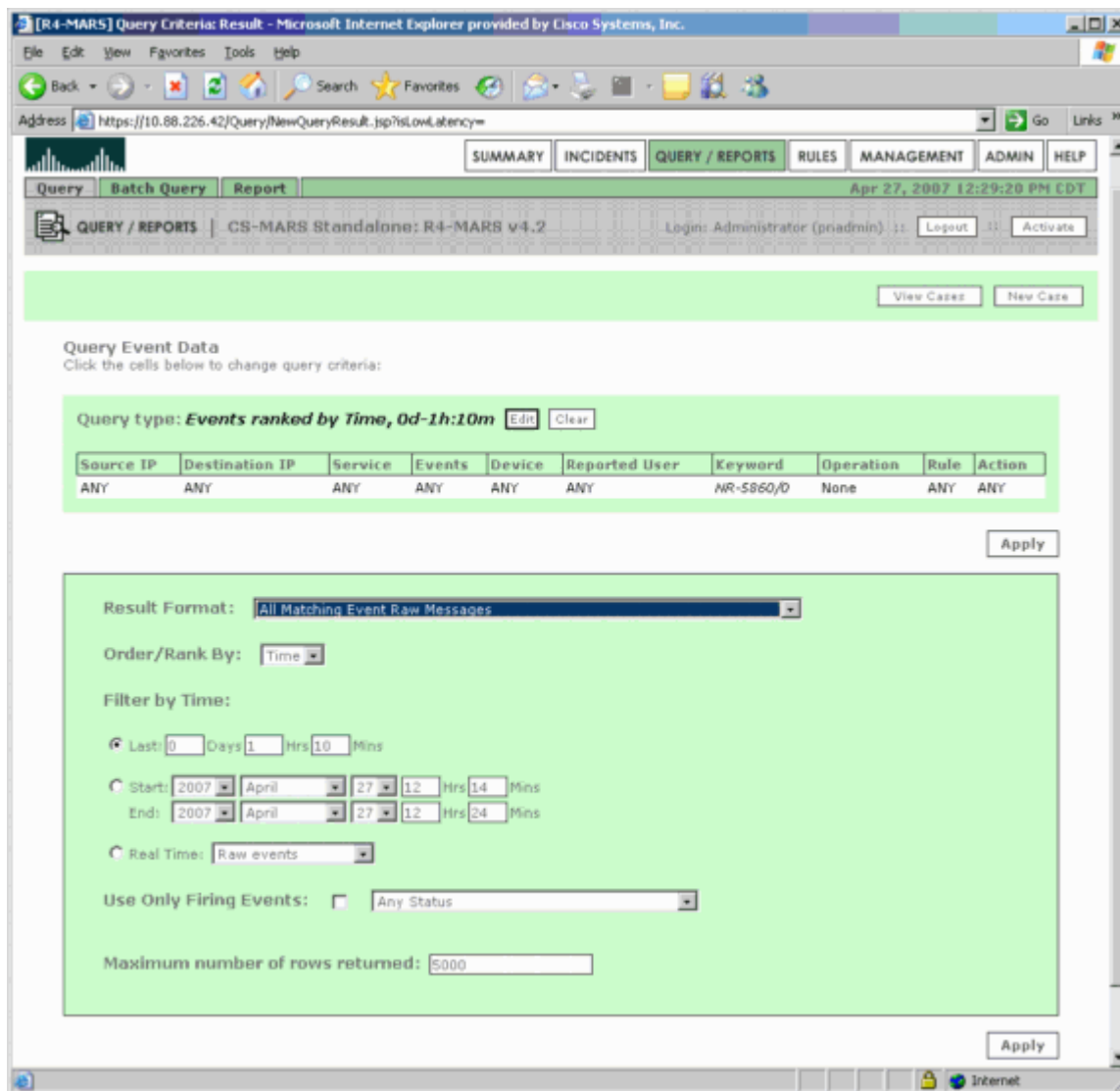
```
signature: description=IOS FTPd Successful Login id=5860 version=S285
  subsigId: 0
  sigDetails: IOS FTPd Successful Login
  marsCategory: Info/SuccessfulLogin/FTP
  marsCategory: Penetrate/ViewFiles/DirTraversal/FTP
interfaceGroup: vs0
vlan: 0
participants:
  attacker:
    addr: locality=OUT 192.168.208.63
    port: 35804
  target:
    addr: locality=OUT 192.168.134.21
    port: 21
    os: idSource=unknown relevance=unknown type=unknown
triggerPacket:
--      Output Truncated      --
riskRatingValue: targetValueRating=medium 42
threatRatingValue: 42
interface: ge0_0
protocol: tcp
```

Cisco Security Monitoring, Analysis, and Response System

Identification: CS MARS Keyword Query

The Cisco Security Monitoring, Analysis, and Response System (Cisco Security MARS) console can be monitored for attempts to exploit the improper authorization checking in IOS FTP server vulnerability.

Using a query with keyword equal **NR-5860/0** and *All Matching Event Raw Messages* result format query on the Cisco Security MARS appliance, events triggered by Signature 5860/0> will be displayed:



The display shown below is the result of the previous query for IPS events triggered by signature 5860/0:

Address: https://10.88.226.42/Query/QuerySubmit.jsp?ResubmitAndClearFaging=true&inlineReport=1

CISCO SYSTEMS

SUMMARY INCIDENTS QUERY / REPORTS RULES MANAGEMENT ADMIN HELP

Query Batch Query Report Summary Apr 27, 2007 12:31:56 PM CDT

QUERY / REPORTS | CS-MARS Standalone: R4-MARS v4.2 Login: Administrator (padmin) :: Logout :: Activate

View Cases New Case

Load Report as On-Demand Query with Filter

Select Group...
Select Report...

Incident ID: Show
Session ID: Show

Query Event Data
Click the cells below to change query criteria:

Query type: *Event Raw Messages ranked by Time, 0d-1h:10m* Edit Clear

Source IP	Destination IP	Service	Events	Device	Reported User	Keyword	Operation	Rule	Action
ANY	ANY	ANY	ANY	ANY	ANY	NR-5860/D	None	ANY	ANY

Save As Report Save As Rule Submit

Query Results

Event / Session / Incident ID	Event Type	Time	Reporting Device	Raw Message	Path / Mitigation	Tune
E:19790312, S:19790312	Unknown Device Event Type [a]	Apr 27, 2007 12:21:55 PM CDT	R4-IPS4240a	192.168.206.63/35812 --> 192.166.128.21/21 TCP Unknown Device Event Type: [a] Time:1177694515,Risk Rating:42,VLAN:0,Port List:21	[a] [b]	False Positive
E:19790317, S:19790317	Unknown Device Event Type [a]	Apr 27, 2007 12:21:55 PM CDT	R4-IPS4240a	192.168.206.63/35812 --> 192.166.128.21/21 TCP Unknown Device Event Type: [a] Time:1177694515,Risk Rating:42,VLAN:0,Port List:21	[a] [b]	False Positive

Address: https://10.88.226.42/Summary/index.jsp?NewQuery=clearReport

Additional Information

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.

Revision History

Revision 1.1	2007-May-11	Include CVE names assigned to vulnerabilities.
Revision 1.0	2007-May-09	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>.

Related Information

- [Protecting Your Core: Infrastructure Protection Access Control Lists](#)
- [Transit Access Control Lists: Filtering at Your Edge](#)
- [Cisco IOS NetFlow](#)
- [Cisco IOS NetFlow White Papers](#)
- [Cisco Network Foundation Protection White Papers](#)
- [Cisco Network Foundation Protection Presentations](#)
- [Cisco Firewall Products](#)
- [Cisco 6.x Intrusion Prevention System](#)
- [Cisco IPS Risk Rating Explained](#)
- [Cisco IPS 6.x Signature Downloads](#) ([registered](#) customers only)

Help us help you.

Please rate this document.

- Excellent
 Good
 Average
 Fair
 Poor

This document solved my problem.

- Yes
 No
 Just browsing

Suggestions for improvement:

(256 character limit)

[Home](#)

[How to Buy](#)

[Login](#)

[Profile](#)

[Feedback](#)

[Site Map](#)

[Help](#)

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2007 - 2008 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)