

# Cisco Applied Mitigation Bulletin: Identifying and Mitigating Exploitation of the CiscoWorks TFTP Directory Traversal Vulnerability

<http://www.cisco.com/warp/public/707/cisco-amb-20090520-cw.shtml>

## Revision 1.0

For Public Release 2009 May 20 1600 UTC (GMT)

---

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

---

## Contents

[Cisco Response](#)

[Device-Specific Mitigation and Identification](#)

[Additional Information](#)

[Revision History](#)

[Cisco Security Procedures](#)

[Related Information](#)

---

## Cisco Response

This Applied Mitigation Bulletin is a companion document to the PSIRT Security Advisory *CiscoWorks TFTP Directory Traversal Vulnerability* and provides identification and mitigation techniques that administrators can deploy on Cisco network devices.

## Vulnerability Characteristics

CiscoWorks Common Services contains a vulnerability that could allow a remote, unauthenticated attacker to access application and host operating system files. This vulnerability can be exploited remotely without authentication and without end-user interaction. Successful exploitation of this vulnerability may allow arbitrary code execution or information disclosure, which could enable an attacker to learn information about the affected device or network. Attempts to exploit this vulnerability could result in a denial of service condition. The attack vector for exploitation is

through TFTP packets using UDP port 69.

This vulnerability has been assigned CVE identifier CVE-2009-1161.

Information about vulnerable, unaffected, and fixed software is available in the PSIRT Security Advisory, which is available at the following link: <http://www.cisco.com/warp/public/707/cisco-sa-20090520-cw.shtml>.

## Mitigation Technique Overview

Cisco devices provide several countermeasures for this vulnerability. Administrators are advised to consider these protection methods to be general security best practices for infrastructure devices and the traffic that transits the network. This section of the document provides an overview of these techniques.

Cisco IOS Software can provide effective means of exploit prevention using infrastructure access control lists (iACLs). This protection mechanism filters and drops packets that are attempting to exploit this vulnerability.

Effective exploit prevention can also be provided by the Cisco ASA 5500 Series Adaptive Security Appliance, the Cisco PIX 500 Series Security Appliance, and the Firewall Services Module (FWSM) for Cisco Catalyst 6500 Series switches and Cisco 7600 Series routers using transit access control lists (tACLs). This protection mechanism filters and drops packets that are attempting to exploit this vulnerability.

Effective use of Cisco Intrusion Prevention System (IPS) event actions provides visibility into and protection against attacks that attempt to exploit this vulnerability.

Cisco IOS NetFlow flow records can provide visibility into network-based exploitation attempts.

Cisco IOS Software, Cisco ASA appliances, Cisco PIX security appliances, and FWSM firewalls can provide visibility through syslog messages and the counter values displayed in the output from **show** commands.

The Cisco Security Monitoring, Analysis, and Response System (Cisco Security MARS) appliance can also provide visibility through incidents, queries, and event reporting.

## Risk Management

Organizations are advised to follow their standard risk evaluation and mitigation processes to determine the potential impact of this vulnerability. Triage refers to sorting projects and prioritizing efforts that are most likely to be successful. Cisco has provided documents that can help organizations develop a risk-based triage capability for their information security teams. [Risk Triage for Security Vulnerability Announcements](#) and [Risk Triage and Prototyping](#) can help organizations develop repeatable security evaluation and response processes.

## Device-Specific Mitigation and Identification

**Caution:** The effectiveness of any mitigation technique depends 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 about 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

To protect infrastructure devices and minimize the risk, impact, and effectiveness of direct infrastructure attacks, administrators are advised to deploy infrastructure access control lists (iACLs) 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 the maximum protection of infrastructure devices, deployed iACLs should be applied in the ingress direction on all interfaces to which an IP address has been configured. An iACL workaround cannot provide complete protection against this vulnerability when the attack originates from a trusted source address.

The iACL policy denies unauthorized TFTP packets on UDP port 69 that are sent to affected devices. In the following example, 192.168.60.0/24 is the IP address space that is used by the affected devices, and the host at 192.168.100.1 is considered a trusted source that requires access to the affected devices. Care should be taken to allow required traffic for routing and administrative access prior to denying all unauthorized traffic. In addition, insure that access is provided to the affected devices from all network devices that require TFTP services. Whenever possible, infrastructure address space should be distinct from the address space used for user and services segments. Using this addressing methodology will assist with the construction and deployment of iACLs.

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

```
ip access-list extended Infrastructure-ACL-Policy

!
!-- Include explicit permit statements for trusted
!-- sources that require access on the vulnerable port
!

permit udp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 69

!
!-- The following vulnerability-specific access control entry
!-- (ACE) can aid in identification of attacks
!

deny udp any 192.168.60.0 0.0.0.255 eq 69

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

```

deny ip any 192.168.60.0 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 interfaces in the ingress direction
!

interface GigabitEthernet0/0
 ip access-group Infrastructure-ACL-Policy 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. Generating these messages could have the undesired effect of increasing CPU utilization on the device. In Cisco IOS Software, ICMP unreachable generation is limited to one packet every 500 milliseconds by default. ICMP unreachable message generation can be disabled using the interface configuration command **no ip unreachables**. ICMP unreachable rate limiting can be changed from the default using the global configuration command **ip icmp rate-limit unreachable *interval-in-ms***.

## Identification: Infrastructure Access Control Lists

After the administrator applies the iACL to an interface, the **show ip access-lists** command will identify the number of TFTP packets on UDP port 69 that have been filtered on interfaces on which the iACL is applied. Administrators should investigate filtered packets to determine whether they are attempts to exploit this vulnerability. Example output for **show ip access-lists Infrastructure-ACL-Policy** follows:

```

router# show ip access-lists Infrastructure-ACL-Policy
Extended IP access list Infrastructure-ACL-Policy
 10 permit udp host 192.168.100.1 192.168.60.0 0.0.0.255 eq tftp
(435 matches)
 20 deny udp any 192.168.60.0 0.0.0.255 eq tftp (13 matches)
 30 deny ip any 192.168.60.0 0.0.0.255 (9 matches)
router#

```

In the preceding example, access list *Infrastructure-ACL-Policy* has dropped **13 TFTP** packets on **UDP** port **69 (tftp)** for access control list entry (ACE) line 20.

For additional information about investigating incidents using ACE counters and syslog events, reference the [Identifying Incidents Using Firewall and IOS Router Syslog Events](#) Applied Intelligence white paper.

Administrators can use Embedded Event Manager to provide instrumentation when specific conditions are met, such as ACE counter hits. The Applied Intelligence white paper [Embedded Event Manager in a Security Context](#) provides additional details about how to use this feature.

## Identification: Access List Logging

The **log** and **log-input** access control list (ACL) option will cause packets that match specific ACEs to be logged. The **log-input** option enables logging of the ingress interface in addition to the packet source and destination IP addresses and ports.

**Caution:** Access control list logging can be very CPU intensive and must be used with extreme caution. Factors that drive the CPU impact of ACL logging are log generation, log transmission, and process switching to forward packets that match log-enabled ACEs.

For Cisco IOS Software, the **ip access-list logging interval** *interval-in-ms* command can limit the effects of process switching induced by ACL logging. The **logging rate-limit** *rate-per-second* [**except** *loglevel*] command limits the impact of log generation and transmission.

The CPU impact from ACL logging can be addressed in hardware on the Cisco Catalyst 6500 Series switches and Cisco 7600 Series routers with Supervisor Engine 720 or Supervisor Engine 32 using optimized ACL logging.

For additional information about the configuration and use of ACL logging, reference the [Understanding Access Control List Logging](#) Applied Intelligence white paper.

## Cisco IOS NetFlow

### Identification: Traffic Flow Identification Using NetFlow Records

Administrators can configure Cisco IOS NetFlow on Cisco IOS routers and switches to aid in the identification of traffic flows that may be attempts to exploit the vulnerability. Administrators are advised to investigate flows to determine whether they are attempts to exploit the vulnerability or whether they are legitimate traffic flows.

```
router# show ip cache flow
IP packet size distribution (32736 total packets):
  1-32   64   96  128  160  192  224  256  288  320  352  384  416
448   480
  .089 .556 .353 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000
  512   544   576 1024 1536 2048 2560 3072 3584 4096 4608
  .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000
```

```
IP Flow Switching Cache, 278544 bytes
 124 active, 3972 inactive, 18349 added
341664 age polls, 0 flow alloc failures
Active flows timeout in 30 minutes
Inactive flows timeout in 15 seconds
```

```
IP Sub Flow Cache, 34056 bytes
 0 active, 1024 inactive, 0 added, 0 added to flow
 0 alloc failures, 0 force free
 1 chunk, 1 chunk added
last clearing of statistics never
```

```
Protocol          Total      Flows    Packets Bytes    Packets Active(Sec)
Idle(Sec)
-----
                Flows      /Sec      /Flow  /Pkt      /Sec      /Flow      /
Flow
```

TCP-WWW 15.4	99	0.0	13	40	0.0	0.0
TCP-BGP 15.3	17517	0.0	1	69	0.0	2.7
TCP-other 15.5	285	0.0	8	40	0.0	0.0
UDP-NTP 15.3	1	0.0	1	29	0.0	0.0
UDP-TFTP 15.5	87	0.0	3	28	0.0	0.0
UDP-other 15.5	206	0.0	10	28	0.0	0.0
ICMP 15.5	30	0.0	39	56	0.0	0.3
Total: 15.3	18225	0.0	1	61	0.0	2.6

SrcIf DstP	Pkts	SrcIPAddress	DstIf	DstIPAddress	Pr	SrcP
Et0/0 4E72	8	192.168.139.166	Et0/1	192.168.206.68	06	F6AF
Et0/0 250E	3	192.168.1.40	Et0/0	192.168.85.93	11	4E50
Et0/0 0050	23	192.168.0.122	Et0/1	192.168.60.113	06	A67B
<b>Et0/0 0045</b>	<b>5</b>	<b>192.168.255.20</b>	<b>Et0/1</b>	<b>192.168.60.255</b>	<b>11</b>	<b>799B</b>
<b>Et0/0 0045</b>	<b>3</b>	<b>192.168.18.15</b>	<b>Et0/1</b>	<b>192.168.60.205</b>	<b>11</b>	<b>A31C</b>
Et0/0 8047	5	192.168.240.104	Et0/0	192.168.37.168	06	0C86
Et0/0 00B3	2	192.0.2.1	Local	192.0.2.2	06	811B
Et0/0 6995	13	192.168.129.180	Et0/0	192.168.92.129	06	CF89
Et0/0 01BB	1	192.168.0.216	Et0/1	192.168.60.233	06	9444
Et0/0 01BB	2	192.168.0.113	Et0/1	192.168.60.140	06	354B
Et0/0 0050	28	192.168.0.208	Et0/1	192.168.60.103	06	059F
Et0/0 01BB	2	192.168.0.198	Et0/1	192.168.60.198	06	A486
Et0/0 8F7C	11	192.168.159.227	Et0/0	192.168.255.250	06	A06C
Et0/0 D644	2	192.168.18.248	Et0/0	192.168.209.2	11	B215
Et0/0 31C2	10	192.168.207.220	Et0/0	192.168.209.35	11	EE87
Et0/0		192.168.0.77	Et0/1	192.168.60.247	06	32EF

```

0050      10
Et0/0      192.168.0.240   Et0/1      192.168.60.20   06 A316
01BB       3
Et0/0     192.168.146.58 Et0/1     192.168.60.214 11 A413
0045     1
Et0/0      192.168.0.227   Et0/1      192.168.60.177   06 DF6C
01BB       2
Et0/0      192.168.0.146   Et0/1      192.168.60.93    06 8E77
01BB       6
Et0/0      192.168.0.127   Et0/1      192.168.60.59    06 0FE9
0050      25
Et0/0     192.168.225.244 Local     192.168.60.1   11 2967
0045     1
Et0/0      192.168.0.76    Et0/1      192.168.60.131   06 2F1E
0050      33
Et0/0     192.168.241.66 Et0/1     192.168.60.203 11 7AC4
0045     3
Et0/0     192.168.208.227 Et0/1     192.168.60.158 11 F81A
0045     4
Et0/0      192.168.253.214 Et0/0      192.168.57.1     06 89C2
6543       3
Et0/0     192.168.88.77  Et0/1     192.168.60.164 11 A0AE
0045     4
Et0/0      192.168.17.123  Et0/0      192.168.244.101  11 9762
C77B       2
Et0/0     192.168.255.69 Et0/1     192.168.60.80  11 0B53
0045     6
Et0/0      192.168.0.53    Et0/1      192.168.60.215   06 082E
0050      30
Et0/0     192.168.163.175 Et0/1     192.168.60.167 11 0B36
0045     2
Et0/0      192.168.174.128 Et0/0      192.168.235.9    11 99AF
B3F1       7
Et0/0      192.168.194.152 Et0/0      192.168.85.59    06 5760
33EA       5
Et0/0      192.168.97.137  Et0/0      192.168.49.202   11 3AAD
D2AD      13
router#

```

In the preceding example, there are multiple flows for **TFTP** on **UDP** port **69** (hex value **0045**).

This traffic is sent to addresses within the 192.168.60.0/24 address block which is used by affected devices. The packets in these flows may be spoofed and may indicate an attempt to exploit this vulnerability. Administrators are advised to compare these flows to baseline utilization for TFTP traffic sent on UDP port 69 and also investigate the flows to determine whether they are sourced from untrusted hosts or networks.

To view only the traffic flows for TFTP packets on UDP 69 (hex value 0045), the command **show ip cache flow | include SrcIf|\_11\_.\*0045** will display the related NetFlow records as shown here:

```
router# show ip cache flow | include SrcIf|_11_.*0045
```

SrcIf	SrcIPaddress	DstIf	DstIPaddress	Pr	SrcP
Et0/0	192.168.255.20	Et0/1	192.168.60.255	11	799B
0045					5
Et0/0	192.168.18.15	Et0/1	192.168.60.205	11	A31C
0045					3
Et0/0	192.168.146.58	Et0/1	192.168.60.214	11	A413
0045					1
Et0/0	192.168.225.244	Local	192.168.60.1	11	2967
0045					1
Et0/0	192.168.241.66	Et0/1	192.168.60.203	11	7AC4
0045					3
Et0/0	192.168.208.227	Et0/1	192.168.60.158	11	F81A
0045					4
Et0/0	192.168.88.77	Et0/1	192.168.60.164	11	A0AE
0045					4
Et0/0	192.168.255.69	Et0/1	192.168.60.80	11	0B53
0045					6
Et0/0	192.168.163.175	Et0/1	192.168.60.167	11	0B36
0045					2

router#

## Cisco ASA, PIX, and FWSM Firewalls

### Mitigation: Transit Access Control Lists

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, administrators are advised to deploy tACLs to perform policy enforcement. Administrators can construct a tACL 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. A tACL workaround cannot provide complete protection against this vulnerability when the attack originates from a trusted source address.

The tACL policy denies unauthorized TFTP packets on UDP port 69 that are sent to affected devices. In the following example, 192.168.60.0/24 is the IP address space that is used by the affected devices, and the host at 192.168.100.1 is considered a trusted source that requires 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 in [Transit Access Control Lists: Filtering at Your Edge](#).

```

!
!-- Include any explicit permit statements for trusted sources
!-- that require access on the vulnerable port
!

access-list tACL-Policy extended permit udp host 192.168.100.1
192.168.60.0 255.255.255.0 eq 69

```

```
!
```

```

!-- The following vulnerability-specific access control entry
!-- (ACE) can aid in identification of attacks
!

access-list tACL-Policy extended deny udp any 192.168.60.0
255.255.255.0 eq 69

!
!-- 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 tACL-Policy extended deny ip any any

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

access-group tACL-Policy in interface outside

```

## Identification: Transit Access Control Lists

After the tACL has been applied to an interface, administrators can use the **show access-list** command to identify the number of TFTP packets on UDP port 69 that have been filtered. Administrators are advised to investigate filtered packets to determine whether they are attempts to exploit this vulnerability. Example output for **show access-list tACL-Policy** follows:

```

firewall# show access-list tACL-Policy
access-list tACL-Policy; 3 elements
access-list tACL-Policy line 1 extended permit udp host 192.168.100.1
192.168.60.0 255.255.255.0 eq tftp (hitcnt=50)
access-list tACL-Policy line 2 extended deny udp any 192.168.60.0
255.255.255.0 eq tftp (hitcnt=53)
access-list tACL-Policy line 3 extended deny ip any any (hitcnt=19)
firewall#

```

In the preceding example, access list *tACL-Policy* has dropped **53 TFTP** packets on **UDP port 69 (tftp)** received from an untrusted host or network. 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 IP protocol for the denied packet.

## Identification: Firewall Access List Syslog Messages

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

Information about configuring syslog for the Cisco ASA 5500 Series Adaptive Security Appliance or the Cisco PIX 500

Series Security Appliance is in [Monitoring the Security Appliance - Configuring and Managing Logs](#). Information about configuring syslog on the FWSM for Cisco Catalyst 6500 Series switches and Cisco 7600 Series routers is in [Monitoring the Firewall Services Module](#).

In the following example, the `show logging | grep regex` command extracts syslog messages from the logging buffer on the firewall. These messages provide additional information about denied packets that could indicate potential attempts to exploit the vulnerability that is described in this document. It is possible to use different regular expressions with the `grep` keyword to search for specific data in the logged messages.

Additional information about regular expression syntax is in [Creating a Regular Expression](#).

```
firewall# show logging | grep 106023
Apr 20 2009 16:27:43: %ASA-4-106023: Deny udp src
outside:10.67.42.189/12633
        dst inside:192.168.60.7/69 by access-group "tACL-Policy"
Apr 20 2009 16:27:43: %ASA-4-106023: Deny udp src
outside:10.193.104.28/19615
        dst inside:192.168.60.1/69 by access-group "tACL-Policy"
Apr 20 2009 16:27:43: %ASA-4-106023: Deny udp src
outside:10.156.197.247/34067
        dst inside:192.168.60.31/69 by access-group "tACL-Policy"
Apr 20 2009 16:27:43: %ASA-4-106023: Deny udp src
outside:192.168.155.147/46897
        dst inside:192.168.60.22/69 by access-group "tACL-Policy"
Apr 20 2009 16:27:43: %ASA-4-106023: Deny udp src
outside:10.87.194.109/16790
        dst inside:192.168.60.24/69 by access-group "tACL-Policy"
Apr 20 2009 16:27:43: %ASA-4-106023: Deny udp src
outside:10.161.139.118/26622
        dst inside:192.168.60.10/69 by access-group "tACL-Policy"
firewall#
```

In the preceding example, the messages logged for the tACL *tACL-Policy* show **TFTP** packets for **UDP port 69** sent to the address block assigned to the affected devices.

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

For additional information about investigating incidents using syslog events, reference the [Identifying Incidents Using Firewall and IOS Router Syslog Events](#) Applied Intelligence white paper.

## Cisco Intrusion Prevention System

### Mitigation: Cisco IPS Signature Event Actions

Administrators can use Cisco Intrusion Prevention System (IPS) appliances and services modules to provide threat detection and help prevent attempts to exploit the vulnerability that is described in this document. Beginning with

signature update S256 for sensors running Cisco IPS version 6.x or 5.x, the vulnerability can be detected by signature 5510/0 (Signature Name: Cisco TFTP Directory Traversal). Signature 5510/0 is not enabled by default, triggers a *High* severity event, has a signature fidelity rating (SFR) of 75, and is configured with a default event action of **produce-alert**.

This signature fires when a TFTP request is made by appending a `../` character string to the pathname. Firing of this signature may indicate a potential exploit of the vulnerability, but the nature of the signature may cause it to be triggered by events that are unrelated to exploits of this vulnerability.

Administrators can configure Cisco IPS sensors to perform an event action when an attack is detected. The configured event action performs preventive or deterrent controls to help protect against an attack that is attempting to exploit the vulnerability that is described in this document.

Cisco IPS sensors are most effective when deployed in inline protection mode combined with the use of an event action. Automatic Threat Prevention for Cisco IPS 6.x sensors that are deployed in inline protection mode provides threat prevention against an attack that is attempting to exploit the vulnerability that is described in this document. Threat prevention is achieved through a default override that performs an event action for triggered signatures with a *riskRatingValue* greater than 90.

Cisco IPS 5.x sensors that are deployed in inline protection mode require an event action configured on a per-signature basis. Alternatively, administrators can configure an override that can perform an event action for any signatures that are triggered and are calculated as a high-risk threat. Using an event action on sensors deployed in inline protection mode provides the most effective exploit prevention.

For additional information about the risk rating and threat rating calculation, reference [Risk Rating and Threat Rating: Simplify IPS Policy Management](#).

## Identification: IPS Signature Events

### Signature: 5510/0 Cisco TFTP Directory Traversal

```
IPS# show events alert | include 5510
evIdsAlert: eventId=1238718211601136119 severity=high vendor=Cisco
originator:
  hostId: R3-A041-IPS4240
  appName: sensorApp
  appInstanceId: 428
time: 2009/04/21 16:42:02 2009/04/21 11:42:02 CDT
signature: description=Cisco TFTP Directory Traversal id=5510
created=20050603 type=vulnerability version=S256
subsigId: 0
sigDetails: ../
marsCategory: Info/Misc
interfaceGroup: vs0
vlan: 0
participants:
  attacker:
    addr: locality=OUT 192.168.208.63
    port: 32773
  target:
```

```

addr: locality=OUT 192.168.130.86
port: 69
os: idSource=unknown relevance=relevant type=unknown
triggerPacket:
000000  00 18 73 17 9F E8 00 18  74 B5 A4 1A 08 00 45 00  ..s.....t.....
E.
000010  00 31 00 00 40 00 3F 11  67 D5 C0 A8 D0 3F C0 A8  .1...@.?.
g....?..
000020  82 56 80 05 00 45 00 1D  97 ED 00 01 2E 2E 2F 2E  .V...
E...../..
000030  2E 2F 65 74 63 00 6E 65  74 61 73 63 69 69 00    ./etc.
netascii.
  riskRatingValue: attackRelevanceRating=relevant
targetValueRating=medium 70
  threatRatingValue: 70
  interface: ge0_3
  protocol: udp

```

## Cisco Security Monitoring, Analysis, and Response System

### Identification: Cisco Security Monitoring, Analysis, and Response System Incidents

The Cisco Security Monitoring, Analysis, and Response System (Cisco Security MARS) appliance can create incidents regarding events that are related to the vulnerability that is described in this document using IPS signature 5510/0 (Signature Name: Cisco TFTP Directory Traversal). After the S256 dynamic signature update has been downloaded, using keyword **NR-5510/0** for IPS signature 5510/0 and a query type of **All Matching Event Raw Messages** on the Cisco Security MARS appliance will provide a report that lists the incidents created by the IPS signature.

Beginning with the 4.3.1 and 5.3.1 releases of Cisco Security MARS appliances, support for the Cisco IPS dynamic signature updates feature has been added. This feature downloads new signatures from Cisco.com or from a local web server, correctly processes and categorizes received events that match those signatures, and includes them in inspection rules and reports. These updates provide event normalization and event group mapping, and they also enable the MARS appliance to parse new signatures from the IPS devices.

**Caution:** If dynamic signature updates are not configured, events that match these new signatures appear as *unknown event type* in queries and reports. Because MARS will not include these events in inspection rules, incidents may not be created for potential threats or attacks that occur within the network.

By default, this feature is enabled but requires configuration. If it is not configured, the following Cisco Security MARS rule will be triggered:

```
System Rule: CS-MARS IPS Signature Update Failure
```

When this feature is enabled and configured, administrators can determine the current signature version downloaded by MARS by selecting **Help > About** and reviewing the *IPS Signature Version* value.

Additional information about dynamic signature updates and instructions for configuring dynamic signature updates are available for the Cisco Security MARS [4.3.1](#) and [5.3.1](#) releases.

## 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 1.0	2009-May-20	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](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

- [Cisco Applied Mitigation Bulletins](#)
  - [Cisco Guide to Harden Cisco IOS Devices](#)
  - [Cisco Security Center](#)
  - [Cisco IOS NetFlow - Home Page on Cisco.com](#)
  - [Cisco IOS NetFlow White Papers](#)
  - [NetFlow Performance Analysis](#)
  - [Cisco Network Foundation Protection White Papers](#)
  - [Cisco Network Foundation Protection Presentations](#)
  - [TTL Expiry Attack Identification and Mitigation](#)
  - [A Security-Oriented Approach to IP Addressing](#)
  - [Cisco Firewall Products - Home Page on Cisco.com](#)
  - [Cisco 6.x Intrusion Prevention System](#)
  - [Cisco IPS 6.x Signature Downloads](#)
  - [Cisco IPS Signature Search Page](#)
  - [Cisco Security Monitoring, Analysis, and Response System](#)
  - [Common Vulnerabilities and Exposures \(CVE\)](#) 
-

## 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](#)

© 2008 - 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)