

Cisco Applied Mitigation Bulletin: Identifying and Mitigating Exploitation of the Cisco ACE Application Control Engine Device Manager and Application Networking Manager Vulnerabilities

<http://www.cisco.com/warp/public/707/cisco-amb-20090225-anm.shtml>

Revision 1.0

For Public Release 2009 February 25 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 *Cisco ACE Application Control Engine Device Manager and Application Networking Manager Vulnerabilities* and provides identification and mitigation techniques that administrators can deploy on Cisco network devices.

Vulnerability Characteristics

There are multiple vulnerabilities in the Cisco ACE Application Control Engine Device Manager (DM) and Cisco Application Networking Manager (ANM). The following subsections summarize two of these

vulnerabilities that have a network mitigation.

The Cisco ANM MySQL server uses a default administrative password that could permit access to the MySQL database. This vulnerability could be exploited remotely with default credential authentication and without end-user interaction. Successful exploitation of this vulnerability may allow remote unauthorized system access. Modification of Cisco ANM settings or the MySQL database may result in file modification, causing a denial of service (DoS) condition. The attack vector for exploitation is through TCP packets sent to TCP ports that are opened on systems running Cisco ANM.

This vulnerability has been assigned CVE identifier CVE-2009-0617.

The Cisco ANM Java agent contains a vulnerability that opens TCP ports on the Cisco ANM Server, which could permit administrative access to the Cisco ANM server. This vulnerability can be exploited remotely without authentication and without end-user interaction. Successful exploitation of this vulnerability may allow an attacker to stop ANM processes, resulting in a DoS condition or information disclosure. Information disclosure enables an attacker to learn information about the affected device. The attack vector for exploitation is by way of TCP packets that are sent to TCP ports opened on the Cisco ANM Server.

This vulnerability has been assigned CVE identifier CVE-2009-0618.

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-20090225-anm.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 transit access control lists (tACLs).

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 tACLs.

These protection mechanisms filter and drop packets that may be attempting to exploit these vulnerabilities.

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

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

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.

- [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: 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 transit access control lists (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 allows TCP and UDP packets from trusted sources to the affected Cisco ANM Server and its associated applications. Sources that are not listed as trusted are considered untrusted. TCP and UDP packets from untrusted sources are denied. 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.

More specific access list entries can be created using the [Application Networking Manager Ports Reference](#) information in the [User Guide for the Cisco Application Networking Manager 2.0](#). Other versions of Cisco ANM may have slightly different required services and ports, which can be determined by consulting the user guide for the appropriate version of Cisco ANM. Administrators who create more specific access list entries are advised to ensure that return traffic is allowed for connections

initiated by the Cisco ANM and its associated applications.

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

```
!-- Include explicit permit statements for trusted sources
!-- that require access to the Cisco ANM Server and
!-- its associated applications
!
!-- Permit TCP packets from trusted sources
!

access-list 150 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255

!
!-- Permit UDP packets from trusted sources
!-- UDP connections need to be allowed from trusted sources
!-- to the Cisco ANM Server and its associated
!-- applications for full functionality
!

access-list 150 permit udp host 192.168.100.1 192.168.60.0 0.0.0.255

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

access-list 150 deny tcp 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
!
!-- Explicit deny for all other IP traffic
!

access-list 150 deny ip any any

!
!-- Apply tACL to interfaces in the ingress direction
!

interface GigabitEthernet0/0
 ip access-group 150 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 unreachable**. ICMP unreachable rate limiting can be changed from the default using the global configuration command **ip icmp rate-limit unreachable interval-in-ms**.

Identification: Transit Access Control Lists

After the administrator applies the tACL to an interface, the **show ip access-lists** command will identify the number of TCP packets 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 ip access-lists 150** follows:

```
router#show ip access-lists 150
Extended IP access list 150
 10 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 (11 matches)
 20 permit udp host 192.168.100.1 192.168.60.0 0.0.0.255 (1115 matches)
 30 deny tcp any 192.168.60.0 0.0.0.255 (129 matches)
 40 deny ip any any
router#
```

In the preceding example, access list 150 has dropped **129 TCP** packets for access control list entry (ACE) line 30.

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 (90784136 total packets):
```

```

1-32  64  96  128  160  192  224  256  288  320  352  384  416  448  480
.000 .698 .011 .001 .004 .005 .000 .004 .000 .000 .003 .000 .000 .000 .000

512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
.000 .001 .256 .000 .010 .000 .000 .000 .000 .000 .000 .000

```

```
IP Flow Switching Cache, 4456704 bytes
```

```
1885 active, 63651 inactive, 59960004 added
```

```
129803821 aged polls, 0 flow alloc failures
```

```
Active flows timeout in 30 minutes
```

```
Inactive flows timeout in 15 seconds
```

```
IP Sub Flow Cache, 402056 bytes
```

```
0 active, 16384 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-Telnet	11393421	2.8	1	48	3.1	0.0	1.4
TCP-FTP	236	0.0	12	66	0.0	1.8	4.8
TCP-FTPD	21	0.0	13726	1294	0.0	18.4	4.1
TCP-WWW	22282	0.0	21	1020	0.1	4.1	7.3
TCP-X	719	0.0	1	40	0.0	0.0	1.3
TCP-BGP	1	0.0	1	40	0.0	0.0	15.0
TCP-Frag	70399	0.0	1	688	0.0	0.0	22.7
TCP-other	26	0.0	150	40	0.0	0.0	15.5
UDP-DNS	582	0.0	4	73	0.0	3.4	15.4
UDP-NTP	287252	0.0	1	76	0.0	0.0	15.5
UDP-other	310347	0.0	2	230	0.1	0.6	15.9
ICMP	11674	0.0	3	61	0.0	19.8	15.5
IPv6INIP	15	0.0	1	1132	0.0	0.0	15.4
GRE	4	0.0	1	48	0.0	0.0	15.3
Total:	59957957	14.8	1	196	22.5	0.0	1.5

SrcIf	SrcIPAddress	DstIf	DstIPAddress	Pr	SrcP	DstP	Pkts
Gi0/1	192.0.2.53	Gi0/0	192.168.60.52	06	0506	OCEA	496
Gi0/1	192.0.2.53	Gi0/0	192.168.60.52	06	0506	AD40	479
Gi0/0	192.168.10.201	Gi0/1	192.168.60.102	11	0984	00A1	1
Gi0/1	192.0.2.41	Gi0/0	192.168.60.72	06	058A	AD3F	1
Gi0/1	192.0.2.186	Gi0/0	192.168.60.12	06	0989	C364	228
Gi0/1	192.0.2.2	Gi0/0	192.168.60.13	06	16DE	9C86	469
Gi0/0	10.89.16.226	Gi0/1	192.168.150.60	06	12CA	0016	1
Gi0/1	192.0.2.48	Gi0/0	192.168.60.71	06	0506	1F98	1
Gi0/1	192.0.2.89	Gi0/0	192.168.60.75	06	10E7	9DD1	121
Gi0/0	192.168.11.54	Gi0/1	192.168.60.158	11	0911	00A1	3
Gi0/1	192.0.2.2	Gi0/0	192.168.60.13	06	16DE	EA63	473
Gi0/1	192.0.2.129	Gi0/0	192.168.60.74	06	096C	0694	1
Gi0/0	192.168.12.185	Gi0/1	192.168.60.239	11	0BD7	00A1	1
Gi0/1	192.0.2.129	Gi0/0	192.168.60.74	06	096C	2731	1
Gi0/0	192.168.10.17	Gi0/1	192.168.60.97	11	0B89	00A1	1
Gi0/1	192.0.2.101	Gi0/0	192.168.60.11	06	0718	A9B1	151
Gi0/1	192.0.2.213	Gi0/0	192.168.60.73	06	054A	A570	1
Gi0/1	192.0.2.53	Gi0/0	192.168.60.52	06	0506	A564	477

```

Gi0/1      192.0.2.48      Gi0/0      192.168.60.71    06 0506 A56F      1
Gi0/1      192.168.150.60   Gi0/0      10.89.16.226     06 0016 12CA      1
Gi0/1      192.0.2.186     Gi0/0      192.168.60.12   06 0989 EA62     228
Gi0/1      192.0.2.101     Gi0/0      192.168.60.11   06 0718 157D     151
Gi0/1      192.0.2.213     Gi0/0      192.168.60.73   06 054A 0693      1
Gi0/1      192.0.2.186     Gi0/0      192.168.60.12   06 0989 9C72     228
Gi0/1      192.0.2.89      Gi0/0      192.168.60.75   06 10E7 A571     121
Gi0/1      192.0.2.101     Gi0/0      192.168.60.11   06 0718 C350     151
Gi0/0      192.168.13.97   Gi0/1      192.168.60.28   11 0B3E 00A1      5
Gi0/1      192.0.2.48      Gi0/0      192.168.60.71   06 0506 01BB      1
Gi0/1      192.0.2.129     Gi0/0      192.168.60.74   06 096C AD40      1
Gi0/0      10.88.226.1     Gi0/1      192.168.202.22  11 007B 007B      1
Gi0/1      192.0.2.213     Gi0/0      192.168.60.73   06 054A 2331      1
Gi0/1      192.0.2.41      Gi0/0      192.168.60.72   06 058A 0202      1
Gi0/1      192.0.2.89      Gi0/0      192.168.60.75   06 10E7 06CD     121
Gi0/1      192.0.2.48      Null       192.168.0.5      06 0506 01BB      1
Gi0/1      192.0.2.48      Null       192.168.0.6      06 0506 01BB      1
Gi0/1      192.0.2.48      Null       192.168.0.3      06 0506 01BB      1
Gi0/1      192.0.2.48      Null       192.168.0.4      06 0506 01BB      1
Gi0/1      192.0.2.48      Null       192.168.0.1      06 0506 01BB      1
Gi0/1      192.0.2.48      Null       192.168.0.2      06 0506 01BB      1
Gi0/1      192.0.2.48      Null       192.168.0.9      06 0506 01BB      1
Gi0/1      192.0.2.48      Null       192.168.0.7      06 0506 01BB      1
Gi0/1      192.0.2.48      Null       192.168.0.8      06 0506 01BB      1
router#

```

In the preceding example, there are multiple flows for **TCP** packets that are sent to the 192.168.60.0 address block.

To view only the traffic flows for TCP packets sent to the 192.168.60.0 address block, the command **show ip cache flow | include SrcIf|192\168\60\..+_06_** will display the related TCP NetFlow records as shown here.

```

router#show ip cache flow | include SrcIf|192\168\60\..+_06_
SrcIf      SrcIPAddress      DstIf      DstIPAddress      Pr SrcP DstP      Pkts
Gi0/1      192.0.2.53        Gi0/0      192.168.60.52    06 0506 0CEA     493
Gi0/1      192.0.2.53        Gi0/0      192.168.60.52    06 0506 AD40     486
Gi0/1      192.0.2.41        Gi0/0      192.168.60.72    06 058A AD3F      1
Gi0/1      192.0.2.186       Gi0/0      192.168.60.12    06 0989 C364     228
Gi0/1      192.0.2.2         Gi0/0      192.168.60.13    06 16DE 9C86     470
Gi0/1      192.0.2.48        Gi0/0      192.168.60.71    06 0506 1F98      1
Gi0/1      192.0.2.89        Gi0/0      192.168.60.75    06 10E7 9DD1     121
Gi0/1      192.0.2.2         Gi0/0      192.168.60.13    06 16DE EA63     475
Gi0/1      192.0.2.129       Gi0/0      192.168.60.74    06 096C 0694      1
Gi0/1      192.0.2.129       Gi0/0      192.168.60.74    06 096C 2731      1
Gi0/1      192.0.2.101       Gi0/0      192.168.60.11    06 0718 A9B1     151
Gi0/1      192.0.2.213       Gi0/0      192.168.60.73    06 054A A570      1
Gi0/1      192.0.2.53        Gi0/0      192.168.60.52    06 0506 A564     485
Gi0/1      192.0.2.48        Gi0/0      192.168.60.71    06 0506 A56F      1
Gi0/1      192.0.2.186       Gi0/0      192.168.60.12    06 0989 EA62     228
Gi0/1      192.0.2.101       Gi0/0      192.168.60.11    06 0718 157D     151
Gi0/1      192.0.2.213       Gi0/0      192.168.60.73    06 054A 0693      1
Gi0/1      192.0.2.186       Gi0/0      192.168.60.12    06 0989 9C72     228
Gi0/1      192.0.2.89        Gi0/0      192.168.60.75    06 10E7 A571     121
Gi0/1      192.0.2.101       Gi0/0      192.168.60.11    06 0718 C350     151
Gi0/1      192.0.2.48        Gi0/0      192.168.60.71    06 0506 01BB      1
Gi0/1      192.0.2.129       Gi0/0      192.168.60.74    06 096C AD40      1
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 allows TCP and UDP connections from trusted sources to the affected Cisco ANM Server and its associated applications. Sources that are not listed as trusted are considered untrusted. TCP and UDP connections from untrusted sources are denied. 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.

More specific access list entries can be created using the [Application Networking Manager Ports Reference](#) information in the [User Guide for the Cisco Application Networking Manager 2.0](#). Other versions of Cisco ANM may have slightly different required services and ports, which can be determined by consulting the user guide for the appropriate version of Cisco ANM. Administrators who create more specific access list entries are advised to ensure that return traffic is allowed for connections initiated by the Cisco ANM and its associated applications.

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

```
!-- Include explicit permit statements for trusted sources
!-- that require access to the Cisco ANM Server and
!-- its associated applications
!
!-- Permit TCP packets from trusted sources
!

access-list tACL-Policy extended permit tcp host 192.168.100.1 192.168.60.0 255

!
!-- Permit UDP packets from trusted sources
!-- UDP connections need to be allowed from trusted sources
!-- to the Cisco ANM Server and its associated
!-- applications for full functionality
!

access-list tACL-Policy extended permit udp host 192.168.100.1 192.168.60.0 255

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

access-list tACL-Policy extended deny tcp any 192.168.60.0 255.255.255.0
```

```

!
!-- 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 TCP packets 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; 4 elements
access-list tACL-Policy line 1 extended permit tcp host 192.168.100.1 192.168.6
access-list tACL-Policy line 2 extended permit udp host 192.168.100.1 192.168.6
access-list tACL-Policy line 3 extended deny tcp any 192.168.60.0 255.255.255.0
access-list tACL-Policy line 4 extended deny ip any any (hitcnt=0)
firewall#

```

In the preceding example, access list *tACL-Policy* has dropped **152 TCP** packets 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
Feb 25 2009 00:15:13: %ASA-4-106023: Deny tcp src outside:192.0.2.18/2944
    dst inside:192.168.60.191/443 by access-group "tACL-Policy"
Feb 25 2009 00:15:13: %ASA-4-106023: Deny tcp src outside:192.2.0.200/2945
    dst inside:192.168.60.33/514 by access-group "tACL-Policy"
Feb 25 2009 00:15:13: %ASA-4-106023: Deny tcp src outside:192.0.2.99/2946
    dst inside:192.168.60.240/1683 by access-group "tACL-Policy"
Feb 25 2009 00:15:13: %ASA-4-106023: Deny tcp src outside:192.0.2.100/2947
    dst inside:192.168.60.115/1684 by access-group "tACL-Policy"
Feb 25 2009 00:15:13: %ASA-4-106023: Deny tcp src outside:192.0.2.88/2949
    dst inside:192.168.60.38/1741 by access-group "tACL-Policy"
Feb 25 2009 00:15:13: %ASA-4-106023: Deny tcp src outside:192.0.2.175/2950
    dst inside:192.168.60.250/3306 by access-group "tACL-Policy"
firewall#
```

In the preceding example, the messages logged for the tACL *tACL-Policy* show **TCP** packets sent to the address block are assigned to 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 one of these vulnerabilities. Beginning with signature update S384 for sensors running Cisco IPS version 6.x or 5.x, one of these vulnerabilities can be detected by signature 15493/0 (Signature Name: Cisco ANM Java Agent Privilege Escalation). Signature 15493/0 is enabled by default, triggers a *Medium* severity event, has a signature fidelity rating (SFR) of 85, and is configured with a default event action of **Produce Alert**.

This signature fires upon detecting an attempt to exploit the Java Agent Privilege Escalation vulnerability in Cisco Application Networking Manager (ANM). Firing of this signature may indicate a potential exploit 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 vulnerabilities that are 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 vulnerabilities that are 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](#)

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 vulnerabilities that are described in this document using IPS signature 15493/0 (Signature Name: Cisco ANM Java Agent Privilege Escalation). After the S384 dynamic signature update has been downloaded, using keyword **NR-15493** for IPS signature 15493/0 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-February-25	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

- [Cisco Applied Mitigation Bulletins](#)
- [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](#)
- [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](#) ([registered](#) customers only)
- [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)



Send

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.](#)