

# Cisco Applied Mitigation Bulletin: Identifying and Mitigating Exploitation of the Multiple Vulnerabilities in Cisco Secure Access Control Server

<http://www.cisco.com/warp/public/707/cisco-amb-20070105-csacs.shtml>

## Revision 1.1

For Public Release 2007 January 10 2200 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

### Vulnerability Characteristics

There are three (3) categories of vulnerabilities (consisting of a total of five (5) vulnerabilities) associated with this Applied Mitigation Bulletin (AMB) document and the corresponding Cisco PSIRT Advisory. The three categories are as follows:

1. Specially Crafted HTTP GET Request Vulnerability: Processing a specially crafted HTTP GET request may crash the CSAdmin service. This vulnerability is also susceptible to a stack overflow condition.  
There is one vulnerability within this category that can be exploited remotely with no authentication and no user interaction is necessary. If exploited, the attacker may perform remote code execution on the Cisco Secure (CS) Access Control Server (ACS) server/appliance. The attack vector is through the HTTP/HTTPS port (TCP/2002) configured for administration of the ACS device. This vulnerability is not covered by a CVE ID.
2. Specially Crafted RADIUS Accounting-Request Vulnerability: Processing a specially crafted

RADIUS Accounting-Request packet may crash the CSRADIUS service. This vulnerability is also susceptible to a stack overflow condition.

There is one vulnerability within this category that can be exploited remotely with authentication and no user interaction is necessary. If exploited, the attacker may perform remote code execution on the CS ACS server/appliance and may create a Denial of Service (DoS). The attack vector is through the sending of RADIUS Accounting-Request packets using UDP port 1646 or UDP port 1813. In order for the exploit to be successful the source IP of the attacker must be configured (either explicitly or using wildcard IP addressing) as a Network Access Server (NAS) device within ACS. For production environments where RADIUS is not required, RADIUS can be disabled in ACS to mitigate this vulnerability. This vulnerability is covered by CVE ID 2006-4098.

3. Specially Crafted RADIUS Access-Request Vulnerabilities: Processing a specially crafted RADIUS Access-Request packet may crash the CSRADIUS service.

There are three (3) vulnerabilities within this category that can be exploited remotely with no authentication and no user interaction is necessary. If exploited, the attacker may create a Denial of Service (DoS). The attack vector is through the sending of RADIUS Access-Request packets using UDP port 1645 or UDP port 1812. In order for the exploit to be successful the source IP of the attacker must be configured (either explicitly or using wildcard IP addressing) as a Network Access Server (NAS) device within ACS. For production environments where RADIUS is not required, RADIUS can be disabled in ACS to mitigate this vulnerability. One of the vulnerabilities is covered by CVE ID 2006-4097 while the remaining two (2) vulnerabilities are not covered by a CVE ID.

This document contains information to assist Cisco customers in mitigating attempts to exploit the Multiple Vulnerabilities in Cisco Secure Access Control Server. Certain versions of Cisco Secure Access Control Server (ACS) for Windows and the Cisco Secure ACS Solution Engine appliance are affected by multiple vulnerabilities that cause specific Cisco Secure services to crash. Two of the vulnerabilities may permit arbitrary code execution after exploitation of the specified vulnerability.

Vulnerable, non-affected and fixed software information is available in the PSIRT Security Advisory: <http://www.cisco.com/warp/public/707/cisco-amb-20070105-csacs.shtml>

## Mitigation Technique Overview

Cisco devices provide several countermeasures for the Multiple Vulnerabilities in Cisco Secure Access Control Server. The most preventive control is provided by Access Control Lists (ACLs) applied on Cisco IOS software and PIX, ASA, and Firewall Services Module (FWSM) firewalls at the network level. Detective controls can also be performed through the use of Cisco IOS NetFlow, IOS ACLs, and by PIX, ASA, and FWSM Firewalls.

In addition, customers should follow the best practices contained in [Securing ACS Running on Microsoft Windows Platforms](#).

## Device-Specific Mitigation and Identification

- [Internet Edge Routers](#)
- [NetFlow](#)
- [Cisco ASA, PIX, and FWSM Firewalls](#)
- [Cisco Intrusion Prevention System \(IPS\)](#)

- [Cisco Security Monitoring, Analysis, and Response System \(CS MARS\)](#)

## Internet Edge Routers

The Internet Edge router can be used to mitigate and detect attempted exploitation of this issue if access to ACS can be obtained via the public Internet.

### Mitigation



**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.

### Interface Access-lists

Internet Edge routers can be configured with interface access-lists to drop packets that can be used to exploit this issue.

The following access list permits initial HTTP Administration (TCP/2002) packets and the secondary TCP port range (see ACS Note and ACS Configuration Example below) from a trusted management network (i.e. 192.0.2.0/24) destined for the target ACS device (i.e. 192.168.131.100). It also permits RADIUS Authentication (UDP/1645, UDP/1812) and RADIUS Accounting (UDP/1646, UDP/1813) request packets from a network block (192.168.10.0/24) of network devices that will be communicating with ACS over RADIUS (Authentication/Accounting). All other HTTP Administration and RADIUS packets destined to the ACS device are dropped.

```
!-- Allow HTTP (TCP/2002) packets and secondary port range from known
!-- trusted source addresses only to the destination ACS device (192.168.131

access-list 100 permit tcp 192.0.2.0 0.0.0.255 host 192.168.131.100 eq 2002
access-list 100 permit tcp 192.0.2.0 0.0.0.255 host 192.168.131.100 range 11

!-- Allow RADIUS Authentication (UDP/1645, UDP/1812)
!-- and RADIUS Accounting (UDP/1646, UDP/1813)
!-- packets from network device IP address block (192.168.10.0/24).

access-list 100 permit udp 192.168.10.0 0.0.0.255 host 192.168.131.100 eq 16
access-list 100 permit udp 192.168.10.0 0.0.0.255 host 192.168.131.100 eq 16
access-list 100 permit udp 192.168.10.0 0.0.0.255 host 192.168.131.100 eq 18
access-list 100 permit udp 192.168.10.0 0.0.0.255 host 192.168.131.100 eq 18

!-- Block HTTP and RADIUS packets from all other source addresses.

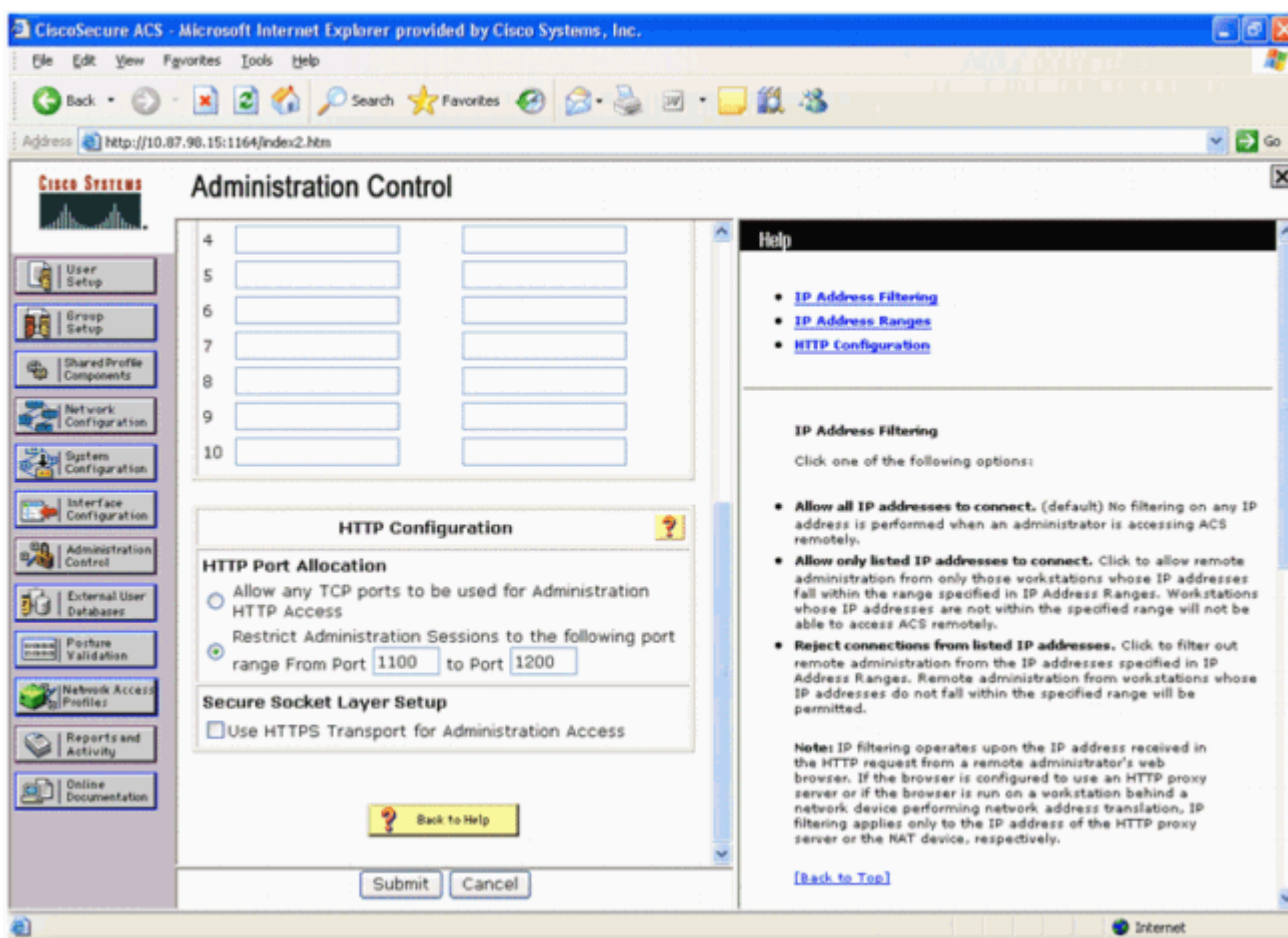
access-list 100 deny tcp any host 192.168.131.100 eq 2002
access-list 100 deny udp any host 192.168.131.100 eq 1645
access-list 100 deny udp any host 192.168.131.100 eq 1646
access-list 100 deny udp any host 192.168.131.100 eq 1812
access-list 100 deny udp any host 192.168.131.100 eq 1813
```

```
!-- Permit/deny all other IP traffic in accordance
!-- with existing security policies and configurations.
!-- Apply access list to interface in the inbound direction.
```

```
interface FastEthernet0
ip access-group 100 in
!
```

**Note:** After the ACS administrative session is initiated over TCP/2002 the ACL above must also permit HTTP traffic over the ACS administrative port range. This port range is configurable (by default all TCP ports are used) within ACS and is described in the [ACS User Guide](#).

In the following ACS configuration example the secondary port range has been restricted to TCP/1100 - TCP/1200 (inclusive). This secondary port range is used in the ACL above and will be used in the configurations throughout the remainder of this document.



These ACL statements may be deployed on the IOS Internet Edge router as part of a transit access-list which will protect the router itself and devices deployed behind it. Further information about transit ACLs is available in the white paper [Transit Access Control Lists: Filtering at Your Edge](#).

Please note that filtering traffic 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 side effect of high CPU utilization since the device needs to generate these ICMP unreachable messages. In IOS, ICMP unreachable generation is limited to one packet per 500 ms. ICMP unreachable generation can be disabled using the interface configuration command **no ip unreachable**. ICMP unreachable rate-limiting can be changed from the default 1 per 500 ms using the global configuration command **ip icmp rate-limit unreachable (1-4294967295 millisecond)**.

Anti-Spoofing - The RADIUS Access-Request and Accounting-Request vulnerabilities can be exploited by a single, easily spoofed packet. Anti-spoof protection in the form of interface access-lists or unicast Reverse Path Forwarding can provide limited mitigation if properly configured. This mitigation should not be relied upon to provide 100% mitigation since spoofed packets may still enter the core from the interface expected by uRPF or allowed by anti-spoofing access-lists. Also care must be taken to ensure that the appropriate uRPF mode (loose or strict) is configured to ensure that legitimate packets are not dropped.

Additional information about unicast Reverse Path Forwarding is available at:  
[http://www.cisco.com/en/US/docs/ios/12\\_2t/12\\_2t13/feature/guide/ft\\_urpf.html](http://www.cisco.com/en/US/docs/ios/12_2t/12_2t13/feature/guide/ft_urpf.html)

## Identification

### Interface Access Lists

Once the interface access list is applied, the **show access-list** command can be used to identify the number of packets being filtered. Filtered packets should be investigated to determine if they are potential attempts to exploit one of the vulnerabilities described within this document. Example output for **show access-list 100**:

```
router-01#show access-list 100
Extended IP access list 100
10 permit tcp 192.0.2.0 0.0.0.255 host 192.168.131.100 eq 2002
20 permit tcp 192.0.2.0 0.0.0.255 host 192.168.131.100 range 1100 1200
30 permit udp 192.168.10.0 0.0.0.255 host 192.168.131.100 eq 1645
40 permit udp 192.168.10.0 0.0.0.255 host 192.168.131.100 eq 1646
50 permit udp 192.168.10.0 0.0.0.255 host 192.168.131.100 eq 1812
60 permit udp 192.168.10.0 0.0.0.255 host 192.168.131.100 eq 1813
70 deny tcp any host 192.168.131.100 eq 2002 (156 matches)
80 deny udp any host 192.168.131.100 eq 1645
90 deny udp any host 192.168.131.100 eq 1646
100 deny udp any host 192.168.131.100 eq 1812 (42 matches)
110 deny udp any host 192.168.131.100 eq 1813 (123 matches)
router-01#
```

In the above example, there were **156 - TCP/2002 packets, 42 - UDP/1812 (RADIUS Authentication), and 123 - UDP/1813 (RADIUS Accounting)** packets dropped by access list 100, which is applied in the inbound direction on interface FastEthernet0.

## NetFlow

NetFlow can be configured on Internet Edge routers to determine if there are potential attempts in progress to exploit one of the vulnerabilities described within this document.

```
router-01#show ip cache flow
IP packet size distribution (86511669 total packets):
  1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  48
  .000 .002 .990 .001 .000 .004 .000 .000 .000 .000 .000 .000 .000 .000 .00
    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, 4456704 bytes
  12 active, 65524 inactive, 614809 added
  17155065 age polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 270472 bytes
```

```

12 active, 16372 inactive, 614809 added, 614809 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(Se
-----	Flows	/Sec	/Flow	/Pkt	/Sec	/Flow	/Flow
TCP-Telnet	3	0.0	141	98	0.0	61.9	10.8
TCP-BGP	191883	0.0	1	69	0.0	4.4	10.6
TCP-other	3741	0.0	2	57	0.0	1.4	13.5
UDP-DNS	2	0.0	5	29	0.0	9.9	15.6
UDP-NTP	159869	0.0	1	75	0.0	0.0	15.4
UDP-TFTP	2	0.0	3	29	0.0	3.7	15.4
UDP-other	258627	0.0	332	78	20.0	28.7	15.4
ICMP	670	0.0	1	88	0.0	0.0	15.4
Total:	614797	0.1	140	78	20.1	13.4	13.9

SrcIf	SrcIPAddress	DstIf	DstIPAddress	Pr	SrcP	DstP	Pk
Fa0/0	10.86.115.214	Fa0/1	192.168.132.100	06	0B53	0016	
Fa0/0	10.86.115.214	Local	192.168.131.101	06	0A55	0016	
Fa0/0	10.64.0.17	Local	192.168.131.101	11	01F4	01F4	1
Fa0/1	192.168.132.100	Fa0/0	10.86.115.214	06	0016	0B53	
Fa0/0	192.168.131.100	Local	192.168.131.101	06	5161	00B3	
Fa0/1	192.168.132.100	Fa0/0	192.168.131.2	11	007B	007B	
Fa0/1	192.168.132.100	Fa0/0	192.168.131.100	11	0714	0714	
Fa0/1	192.168.132.100	Fa0/0	192.168.131.100	11	0715	0715	
Fa0/1	10.86.216.66	Fa0/0	192.168.131.100	06	0a39	07D2	
Fa0/1	10.86.115.216	Fa0/0	192.168.131.100	06	14a2	07D2	
Fa0/1	10.89.236.174	Fa0/0	192.168.131.100	06	1C04	07D2	
Fa0/0	192.168.131.12	Null	192.168.131.31	11	0089	0089	12
Fa0/0	192.168.131.13	Null	192.168.131.255	11	008A	008A	
Fa0/0	192.168.131.2	Fa0/1	192.168.132.100	11	007B	007B	
Fa0/0	192.168.131.11	Local	192.168.131.101	06	0031	2C0F	

```
router#
```

In the above example, there are several TCP/2002 (DstP = Hex 07D2), UDP/1812 (DstP = Hex 0714), and UDP/1813 (DstP = 0715) flows from untrusted IP addresses destined to the ACS device (192.168.131.100). This may indicate an attempt to exploit the vulnerabilities described within this document and should be compared to the baseline utilization of connections using these ports on the production network.

To only view TCP/2002 (Hex 07D2), UDP/1812 (Hex 0714) and UDP/1813 (Hex 0715) flows, the command **show ip cache flow | include SrcIf|07D2|0714|0715** may be used as shown here:

```
router#show ip cache flow | include SrcIf|07D2|0714|0715
```

SrcIf	SrcIPAddress	DstIf	DstIPAddress	Pr	SrcP	DstP	Pk
Fa0/1	192.168.132.100	Fa0/0	192.168.131.100	11	0714	0714	
Fa0/1	192.168.132.100	Fa0/0	192.168.131.100	11	0715	0715	
Fa0/1	10.86.216.66	Fa0/0	192.168.131.100	06	0a39	07D2	5
Fa0/1	10.86.115.216	Fa0/0	192.168.131.100	06	14a2	07D2	7
Fa0/1	10.89.236.174	Fa0/0	192.168.131.100	06	1C04	07D2	1

```
router-01#
```

**Note:** In order to view legacy RADIUS Authentication (UDP/1645) and Accounting (UDP/1646) packets the Hex values used are Hex 066D (Decimal 1645) and Hex 066E (Decimal 1646).

## Cisco ASA, PIX, and FWSM Firewalls

### Mitigation



**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.

Access lists can be configured on PIX/ASA/FWSM firewalls to only allow HTTP Administration (TCP/2002) packets (and the ACS Administrative secondary TCP Port Range) from trusted management networks destined to an ACS device. In addition, access lists can restrict RADIUS Authentication (UDP/1645, UDP/1812) and RADIUS Accounting (UDP/1646, UDP/1813) request packets from a network block (192.168.10.0/24) of network devices that will be communicating with ACS over RADIUS (Authentication/Accounting). All other HTTP Administration and RADIUS packets destined to the ACS device are dropped.

### PIX/ASA 7.x/FWSM

The following access list permits HTTP (TCP/2002) packets and the secondary TCP port range from the 192.0.2.0/24 trusted management network destined to the ACS device (i.e. 192.168.131.100); it also permits RADIUS Authentication (UDP/1645, UDP/1812) and RADIUS Accounting (UDP/1646, UDP/1813) request packets from network devices. All other HTTP Administration, RADIUS Authentication, and RADIUS Accounting packets destined to the ACS device are dropped.

```
access-list ACS remark Allow trusted network to send HTTP (TCP/2002)
packets and the secondary port range
access-list ACS extended permit tcp 192.0.2.0 255.255.255.0 host
192.168.131.100 eq 2002
access-list ACS extended permit tcp 192.0.2.0 255.255.255.0 host
192.168.131.100 range 1100 1200
access-list ACS remark Allow RADIUS Authentication and Accounting
packets from trusted network infrastructure devices
access-list ACS extended permit udp 192.168.10.0 255.255.255.0
host 192.168.131.100 eq radius
access-list ACS extended permit udp 192.168.10.0 255.255.255.0
host 192.168.131.100 eq radius-acct
access-list ACS extended permit udp 192.168.10.0 255.255.255.0
host 192.168.131.100 eq 1812
access-list ACS extended permit udp 192.168.10.0 255.255.255.0
host 192.168.131.100 eq 1813
access-list ACS remark Deny all other HTTP (TCP/2002) traffic to the network
access-list ACS extended deny tcp any host 192.168.131.100 eq 2002
access-list ACS remark Deny all other RADIUS Authentication/Accounting
traffic to the network device
access-list ACS extended deny udp any host 192.168.131.100 eq radius
access-list ACS extended deny udp any host 192.168.131.100 eq radius-acct
access-list ACS extended deny udp any host 192.168.131.100 eq 1812
access-list ACS extended deny udp any host 192.168.131.100 eq 1813
access-list ACS remark Permit/deny all other IP traffic in accordance
with existing security policies and configurations

!-- Apply ACS access list inbound to outside interface.

access-group ACS in interface outside
!
```

**Note:** In the above access list radius and radius-acct refer to the legacy RADIUS ports UDP/1645 and UDP/1646, respectively. Most current implementations of RADIUS now use UDP/1812 (RADIUS Authentication/Authorization) and UDP/1813 (RADIUS Accounting).

## Identification

### PIX/ASA 7.x/FWSM

```
Firewall#show access-list ACS
access-list ACS; 11 elements
access-list ACS line 1 remark Allow trusted network to send HTTP (TCP/2002)
packets and the secondary port range
access-list ACS line 2 extended permit tcp 192.0.2.0 255.255.255.0
host 192.168.131.100 eq 2002 (hitcnt=0) 0xeac09de5
access-list ACS line 3 extended permit tcp 192.0.2.0 255.255.255.0
host 192.168.131.100 range 1100 1200 (hitcnt=0) 0xea90d99a
access-list ACS line 4 remark Allow RADIUS Authentication and
Accounting packets from trusted network infrastructure devices
access-list ACS line 5 extended permit udp 192.168.10.0 255.255.255.0
host 192.168.131.100 eq radius (hitcnt=0) 0x1802392d
access-list ACS line 6 extended permit udp 192.168.10.0 255.255.255.0
host 192.168.131.100 eq radius-acct (hitcnt=0) 0x4a53841b
access-list ACS line 7 extended permit udp 192.168.10.0 255.255.255.0
host 192.168.131.100 eq 1812 (hitcnt=0) 0x3c33ee22
access-list ACS line 8 extended permit udp 192.168.10.0 255.255.255.0
host 192.168.131.100 eq 1813 (hitcnt=0) 0xe4e3c153
access-list ACS line 9 remark Deny all other HTTP (TCP/2002) traffic
to the network device
access-list ACS line 10 extended deny tcp any host 192.168.131.100
eq 2002 (hitcnt=100) 0x1c9ca39c
access-list ACS line 11 remark Deny all other RADIUS Authentication/Accounti:
traffic to the network device
access-list ACS line 12 extended deny udp any host 192.168.131.100 eq radius
(hitcnt=0) 0x7555dafb
access-list ACS line 13 extended deny udp any host 192.168.131.100
eq radius-acct (hitcnt=0) 0xbd11ee3a
access-list ACS line 14 extended deny udp any host 192.168.131.100
eq 1812 (hitcnt=43) 0xfbd671dc
access-list ACS line 15 extended deny udp any host 192.168.131.100
eq 1813 (hitcnt=36) 0x8004d2a6
access-list ACS line 16 remark Permit/deny all other IP traffic in
accordance with existing security policies and configurations
Firewall#
```

3In the above example, **100 - HTTP Administration (TCP/2002)**, **43 - RADIUS Authentication (UDP/1812)** and **36 - RADIUS Accounting (UDP/1813)** packets have been received from a non-trusted host or network and were blocked.

In addition, the following PIX/ASA syslog message will be sent for any attempts that are blocked by access list ACS:

```
Dec 3 2006 15:08:55: %ASA-4-106023: Deny tcp src outside:10.89.236.157/32782
dst inside:192.168.131.100/2002 by access-group "ACS"
```

For more information, refer to [Cisco Security Appliance System Log Message 106023](#).

In addition, the following FWSM syslog message will be sent for any attempts that are blocked by access list ACS:

```
Dec 3 2006 14:13:36: %FWSM-4-106023: Deny tcp src outside:10.89.236.157/3295
dst inside:192.168.131.100/2002 by access-group "ACS"
```

For more information, refer to [Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Logging Configuration and System Log Message 106023](#).

# Cisco Intrusion Prevention System (IPS)

## Mitigation



**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.

The Cisco Intrusion Prevention System (IPS) can potentially be used to provide identification and threat mitigation of attempts to exploit the Specially Crafted HTTP GET Request Vulnerability and the Specially Crafted RADIUS Accounting-Request Vulnerability starting with signature update S265 for 5.x devices. The HTTP GET Request Vulnerability can be detected using Signature 5830/0 and the RADIUS Accounting-Request Vulnerability can be detected using Signature 5831/0. Signatures 5830/0 and 5831/0 are both enabled by default and each triggers a High severity alarm (see examples below).

In order to trigger preventative controls, IPS signatures 5830/0 and 5831/0 will need to be configured to perform a response action. Response actions that provide this type of mitigation are most effective when using an IPS device that is deployed in inline mode. Attacks attempting to exploit any of the RADIUS vulnerabilities can be successful using spoofed IP addresses.

**Note:** In order to address false positive alarms with Signature 5831/0 (RADIUS Accounting-Request Vulnerability) it is recommended that customers upgrade to Cisco IPS signature update S269 or later.

## Identification

IPS signature 5830/0 triggers a High severity alarm on potential attempts to exploit the Crafted HTTP GET Request Vulnerability which may indicate a remote code execution attack.

The following high severity event was triggered by signature 5830/0 after a potential attempt to exploit the Crafted HTTP GET Request Vulnerability on the target victim at IP address 10.87.98.15:

```
R1-IDSM2#show events alert | include id=5830

evIdsAlert: eventId=1164180515640493516 severity=high vendor=Cisco
  originator:
    hostId: R1-IDSM2
    appName: sensorApp
    appInstanceId: 28153
  time: 2007/01/08 14:59:29 2007/01/08 08:59:29 CST
  signature: description=Cisco Secure Access Control Server HTTP Request Over
    subsigId: 0
    sigDetails: Cisco Secure Access Control Server HTTP Request Overflow
  interfaceGroup:
  vlan: 200
  participants:
    attacker:
      addr: locality=OUT 192.168.150.60
      port: 53722
    target:
      addr: locality=OUT 10.87.98.15
      port: 2002
  context:
    fromAttacker:
```

--- Output Truncated ---

IPS signature 5831/0 triggers a High severity alarm on potential attempts to exploit the Specially Crafted RADIUS Accounting-Request Vulnerability which may indicate a remote code execution attack.

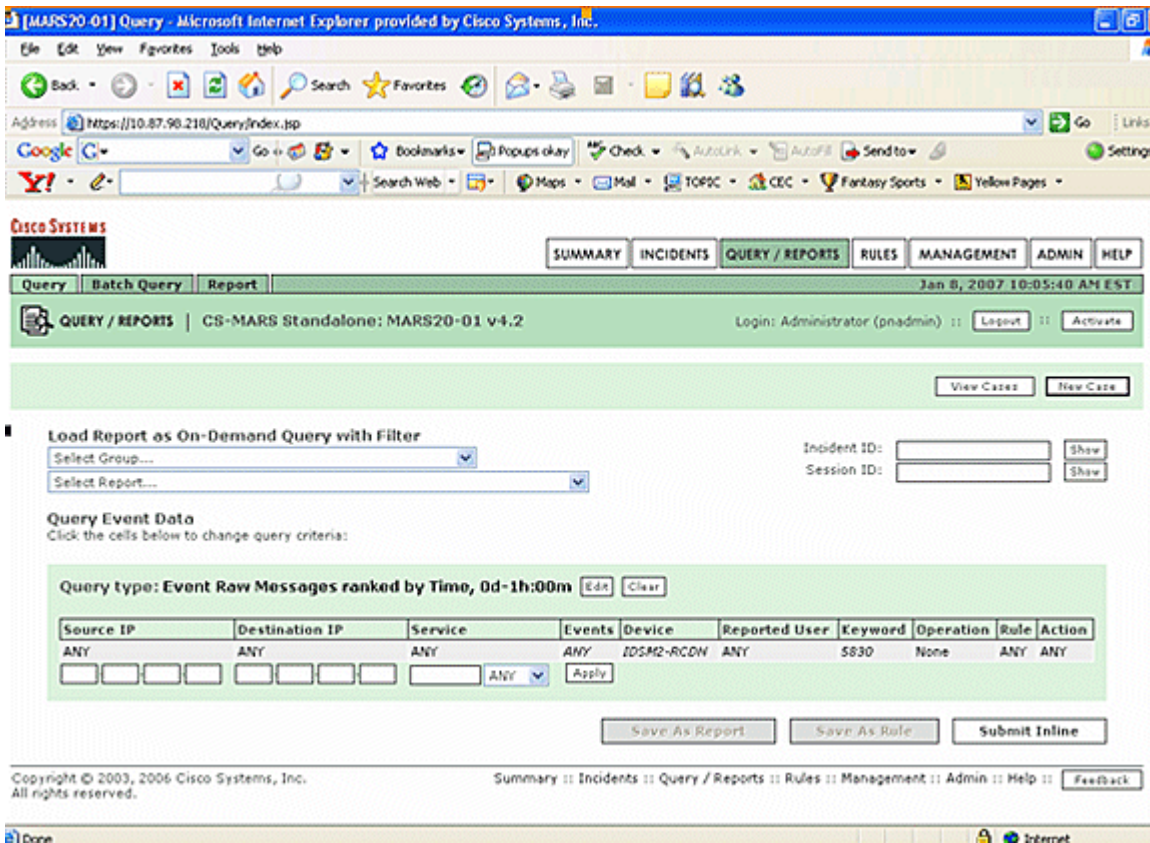
The following high severity event was triggered by signature 5831/0 after a potential attempt to exploit the Specially Crafted RADIUS Accounting-Request Vulnerability on the target victim at IP address 10.87.98.15:

```
R1-IDSM2#show events alert | include id=5831
evIdsAlert: eventId=1164180515640495359 severity=high vendor=Cisco
originator:
  hostId: R1-IDSM2
  appName: sensorApp
  appInstanceId: 28153
time: 2007/01/08 17:24:12 2007/01/08 11:24:12 CST
signature: description=Cisco Secure Access Control Server RADIUS Accountin.
  subsigId: 0
  sigDetails: Cisco Secure Access Control Server RADIUS Accounting Request
interfaceGroup:
vlan: 200
participants:
  attacker:
    addr: locality=OUT 192.168.150.60
    port: 32777
  target:
    addr: locality=OUT 10.87.98.15
    port: 1646
triggerPacket:
--- Output Truncated ---
```

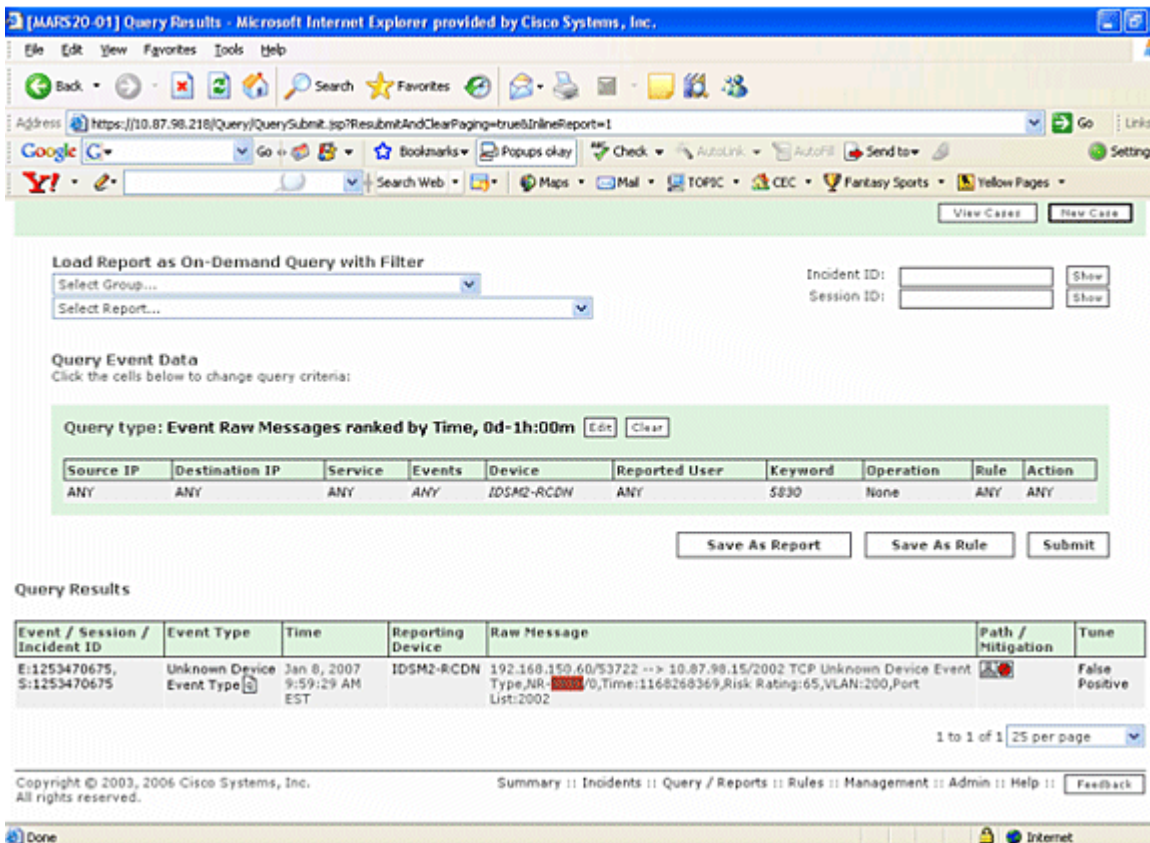
## Cisco Security Monitoring, Analysis, and Response System (CS MARS)

### Identification

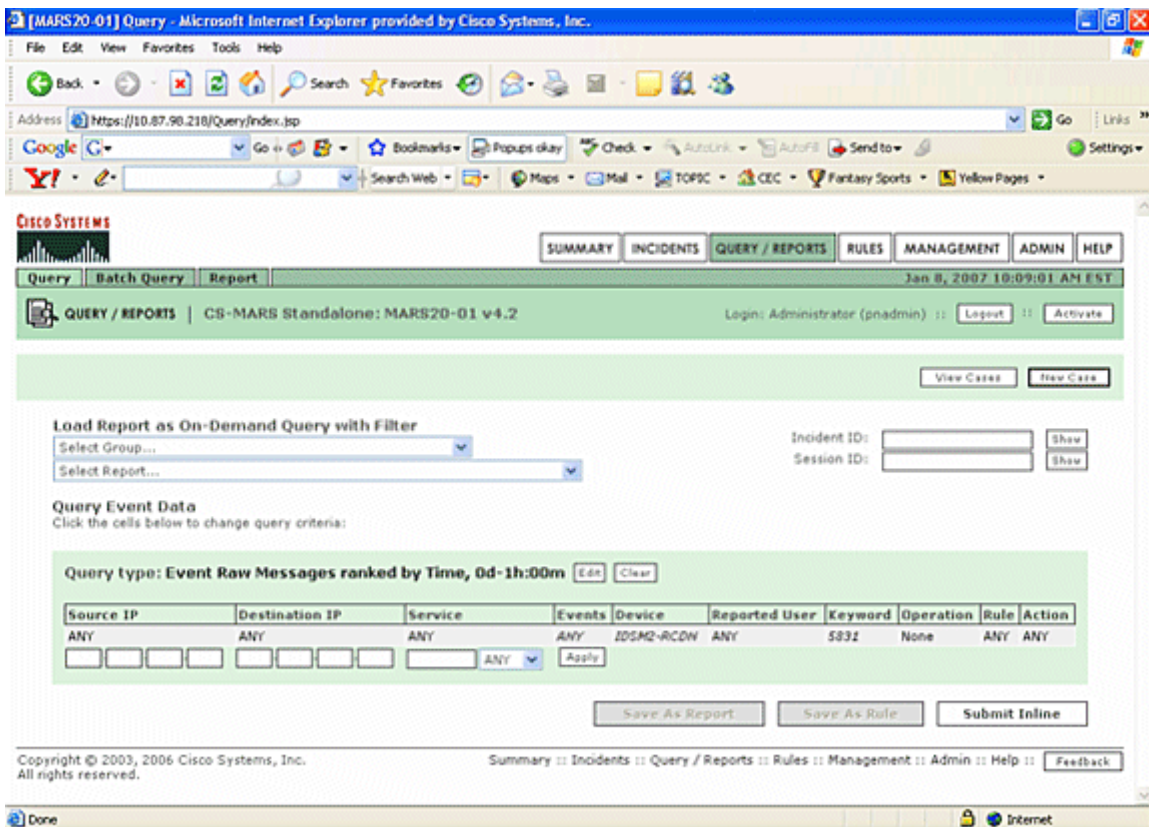
The Cisco Security Monitoring, Analysis, and Response System (Cisco Security MARS) console can be monitored for attempts to exploit the Specially Crafted HTTP GET Request and the Specially Crafted RADIUS Accounting-Request vulnerabilities. Using the following query on the Cisco Security MARS appliance, events triggered by signature 5830/0 will be displayed:



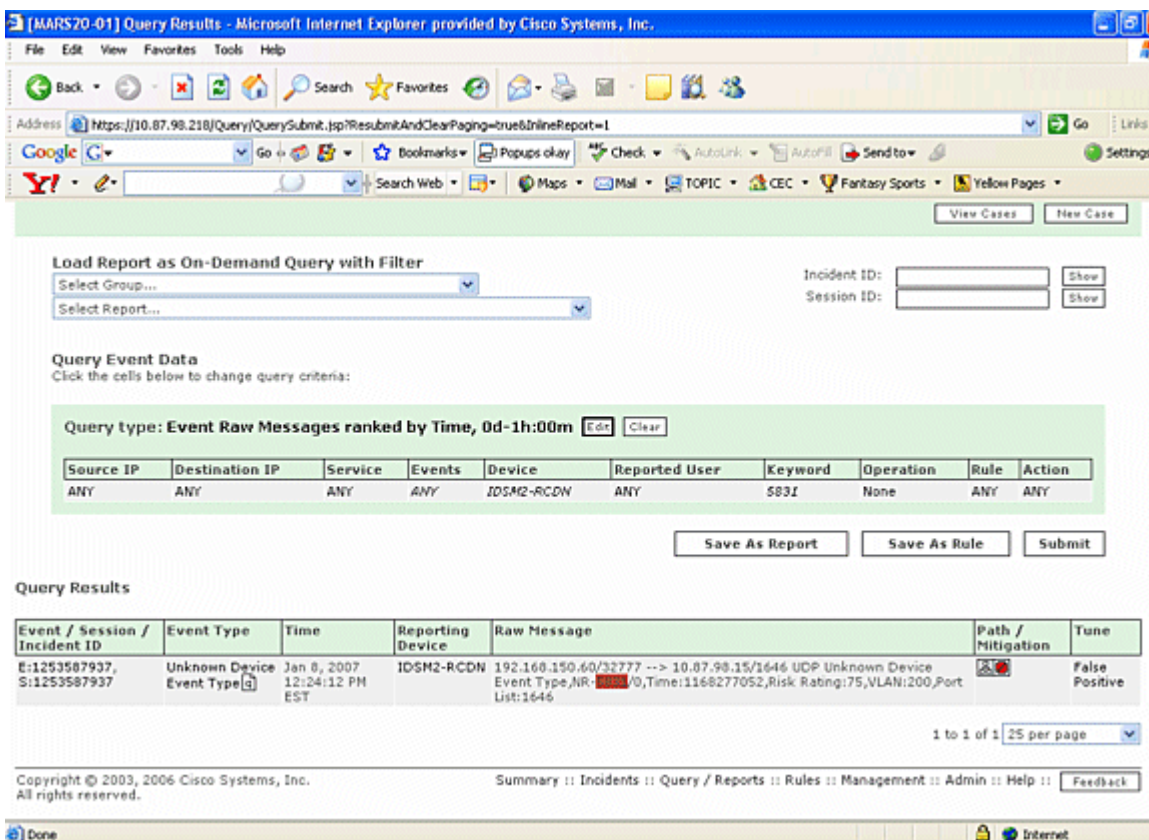
The display shown below is the result of the previous query for IPS events triggered by signature 5830/0:



Using the following query on the Cisco Security MARS appliance, events triggered by signature 5831/0 will be displayed:



The display shown below is the result of the previous query for IPS events triggered by signature 5831/0:



## 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-January-10	Added new links.
Revision 1.0	2007-January-05	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 Secure ACS for Windows](#)
- [Cisco Secure ACS Solution Engine \(Appliance\)](#)
- [Cisco Intrusion Prevention System \(IPS\)](#)
- [Cisco Security Monitoring, Analysis and Response System \(CS MARS\)](#)
- [Cisco IPS 5.x Signature Downloads](#) ( [registered](#) customers only)
- [Signatures by Release Version](#) ( [registered](#) customers only)
- [MySDN Report ID 5314 - HTTP GET Request Buffer Overflow Vulnerability](#) ( [registered](#) customers only)
- [MySDN Report ID 5315 - Specially Crafted RADIUS Accounting-Request Vulnerability](#) ( [registered](#) customers only)
- [MySDN Report ID 5316 - Access-Request Handling Denial of Service Vulnerability \(CSCse18250\)](#) ( [registered](#) customers only)
- [MySDN Report ID 5317 - Access-Request Handling Denial of Service Vulnerability \(CSCeg04788\)](#) ( [registered](#) customers only)
- [MySDN Report ID 5318 - Access-Request Handling Denial of Service Vulnerability \(CSCeg04666\)](#) ( [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)

Send

<a href="#">Home</a>	<a href="#">How to Buy</a>	<a href="#">Login</a>	<a href="#">Profile</a>	<a href="#">Feedback</a>	<a href="#">Site Map</a>	<a href="#">Help</a>
----------------------	----------------------------	-----------------------	-------------------------	--------------------------	--------------------------	----------------------

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

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