

# Cisco Applied Mitigation Bulletin: Identifying and Mitigating Exploitation of the Cisco Unified Communications Disaster Recovery Framework Command Execution Vulnerability

<http://www.cisco.com/warp/public/707/cisco-amb-20080403-drf.shtml>

## Revision 1.1

Last Updated 2008 April 4 1400 UTC (GMT)

For Public Release 2008 April 03 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 Unified Communications Disaster Recovery Framework Command Execution Vulnerability* and provides identification and mitigation techniques that administrators can deploy on Cisco network devices.

### Vulnerability Characteristics

Cisco Unified Communications products contain a vulnerability that allows remote, unauthenticated users to access the Disaster Recovery Framework (DRF) feature using TCP port 4040. This vulnerability

can be exploited remotely without authentication and without end-user interaction. Successful exploitation of this vulnerability may allow arbitrary command execution or result in a denial of service (DoS) condition. Repeated attempts to exploit this vulnerability could result in a sustained DoS condition. The attack vector for exploitation is through packets using TCP port 4040.

This vulnerability has been assigned CVE identifier CVE-2008-1154.

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-20080403-drf.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 (ACLs). 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 (ACLs). This protection mechanism filters and drops packets that are attempting to exploit this vulnerability.

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

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

## 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 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 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: 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 comes from a trusted source address.

The tACL policy denies unauthorized packets on TCP port 4040 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 available in [Transit Access Control Lists: Filtering at Your Edge](#).

```

!--- Include any explicit permit statements for trusted sources
!--- that require access on the vulnerable port TCP 4040
!

access-list 150 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 4040

!
!--- 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 eq 4040

!
!--- 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 packets on TCP port 4040 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 eq 4040
 20 deny tcp any 192.168.60.0 0.0.0.255 eq 4040 (122 matches)
 30 deny ip any any
router#
```

In the preceding example, access list 150 has dropped **122** packets on **TCP** port **4040** for 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 described in this document that have a network attack vector. 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

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    47861004  11.8        1       211    18.9        0.0         1.3
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
Gi0/0     192.168.10.201  Gi0/1     192.168.60.102  11 0984 00A1  1
Gi0/0     192.168.11.54  Gi0/1     192.168.60.158  11 0911 00A1  3
Gi0/1     192.168.150.60  Gi0/0     10.89.16.226    06 0016 12CA  1
Gi0/0     192.168.13.97  Gi0/1     192.168.60.28  11 0B3E 00A1  5
Gi0/0     192.168.10.17  Gi0/1     192.168.60.97  11 0B89 0FC8  1
```

```

Gi0/0      10.88.226.1      Gi0/1      192.168.202.22  11 007B 007B      1
Gi0/0      192.168.12.185   Gi0/1      192.168.60.239  11 0BD7 0FC8      1
Gi0/0      10.89.16.226     Gi0/1      192.168.150.60  06 12CA 0016      1
router#

```

In the preceding example, there are multiple flows for **TCP port 4040 (hex value 0FC8)**. Administrators are advised to compare these flows to baseline utilization for traffic sent on TCP port 4040 and also investigate the flows to determine whether they are sourced from untrusted hosts or networks.

To view only the traffic flows for packets on TCP port 4040 (hex value 0FC8), the command **show ip cache flow | include SrcIf|\_06\_.\*0FC8** will display the related TCP NetFlow records as shown here:

```

router#show ip cache flow | include SrcIf|_06_.*0FC8
SrcIf      SrcIPAddress      DstIf      DstIPAddress      Pr SrcP DstP  Pkts
Gi0/0      192.168.12.110    Gi0/1      192.168.60.163    06 092A 0FC8      6
Gi0/0      192.168.11.230    Gi0/1      192.168.60.20     06 0C09 0FC8      1
Gi0/0      192.168.11.131    Gi0/1      192.168.60.245    06 0B66 0FC8     18
Gi0/0      192.168.13.7      Gi0/1      192.168.60.162    06 0914 0FC8      1
Gi0/0      192.168.41.86     Gi0/1      192.168.60.27     06 0B7B 0FC8      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 comes from a trusted source address.

The tACL policy denies unauthorized packets on TCP port 4040 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 available in [Transit Access Control Lists: Filtering at Your Edge](#).

```

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

access-list Transit-ACL-Policy extended permit tcp host 192.168.100.1 192.168.6

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

```

```

access-list Transit-ACL-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 Transit-ACL-Policy extended deny ip any any

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

access-group Transit-ACL-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 packets on TCP port 4040 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 Transit-ACL-Policy** follows:

```

firewall#show access-list Transit-ACL-Policy
access-list Transit-ACL-Policy; 3 elements
access-list Transit-ACL-Policy line 1 extended permit tcp host 192.168.100.1 19
access-list Transit-ACL-Policy line 2 extended deny tcp any 192.168.60.0 255.25
access-list Transit-ACL-Policy line 3 extended deny ip any any (hitcnt=8)
firewall#

```

In the preceding example, access list *Transit-ACL-Policy* has dropped **119** packets on **TCP port 4040** 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 available 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 available in [Configuring Logging on the Cisco Security Appliance](#). Information about configuring syslog on the FWSM for Cisco Catalyst 6500 Series switches and Cisco 7600 Series routers is available in [Configuring Monitoring and Logging on the Cisco FWSM](#).

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 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 available in [Using the Command Line Interface](#).

```
firewall#show logging | grep 106023
Feb 21 2007 00:15:13: %ASA-4-106023: Deny tcp src outside:192.168.2.18/2944 dst
inside:192.168.60.191/4040 by access-group "Transit-ACL-Policy"
Feb 21 2007 00:15:13: %ASA-4-106023: Deny tcp src outside:192.168.3.200/2945 ds
inside:192.168.60.33/4040 by access-group "Transit-ACL-Policy"
Feb 21 2007 00:15:13: %ASA-4-106023: Deny tcp src outside:192.168.2.99/2946 dst
inside:192.168.60.240/4040 by access-group "Transit-ACL-Policy"
Feb 21 2007 00:15:13: %ASA-4-106023: Deny tcp src outside:192.168.2.100/2947 ds
inside:192.168.60.115/4040 by access-group "Transit-ACL-Policy"
Feb 21 2007 00:15:13: %ASA-4-106023: Deny tcp src outside:192.168.4.88/2949 dst
inside:192.168.60.38/4040 by access-group "Transit-ACL-Policy"
firewall#
```

In the preceding example, the messages logged for the tACL *Transit-ACL-Policy* show packets for **TCP port 4040** sent to the address block assigned to affected devices.

Additional information about syslog messages for ASA and PIX security appliances is available in [Cisco Security Appliance System Log Messages](#). Additional information about syslog messages for the FWSM is available in [Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Logging Configuration and 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 the Cisco Intrusion Prevention System (IPS) appliances and services modules to provide threat detection and help prevent attempts to exploit the vulnerability described in this document. Starting with signature update S327 for sensors running Cisco IPS version 6.x or 5.x, the vulnerability described in this document can be detected by signature 6936/0 (Signature Name: UCM Disaster Recovery Framework Command Execution). Signature 6936/0 is 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**. Signature 6936/0 fires when a single packet sent using TCP port 4040 is detected. Firing of this signature may indicate a potential exploit of the vulnerability described in this document.

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 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 deployed in inline protection mode provides threat prevention against an attack that is attempting to exploit the vulnerability 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: 6936/0 - UCM Disaster Recovery Framework Command Execution

```
IPS#show events alert | include id=6936

evIdsAlert: eventId=1184140689279556354 severity=high vendor=Cisco
  originator:
    hostId: IPS#
    appName: sensorApp
    appInstanceId: 400
  time: 2008/04/04 02:53:10 2008/04/03 21:53:10 CDT
  signature: description=UCM Disaster Recovery Framework Command Execution id=6
    subSigId: 0
    sigDetails: UCM Disaster Recovery Framework Command Execution
    marsCategory: Penetrate/RemoteCmdExec/Misc
  interfaceGroup: vs0
  vlan: 0
  participants:
    attacker:
      addr: locality=OUT 192.168.150.60
      port: 55162
    target:
      addr: locality=OUT 192.168.208.63
      port: 4040
      os: idSource=learned relevance=relevant type=linux
  triggerPacket:

!--- "triggerPacket" Output Truncated

  riskRatingValue: attackRelevanceRating=relevant targetValueRating=medium 75
  threatRatingValue: 75
  interface: ge0_0
  protocol: tcp

IPS#
```

## 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 on events for the Cisco Unified Communications Disaster Recovery Framework command execution vulnerability using IPS signature 6936/0 (Signature Name: UCM Disaster Recovery Framework Command Execution). After the S327 dynamic signature update has been downloaded, using keyword **NR-6936/0** for IPS signature 6936/0 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.

The following screen shot shows the value(s) used to query for events created by IPS signatures related to these vulnerabilities:

The screenshot displays the Cisco MARS Query/Reports interface. At the top, there are navigation tabs: SUMMARY, INCIDENTS, QUERY / REPORTS (selected), RULES, MANAGEMENT, ADMIN, and HELP. Below these are sub-tabs: Query, Batch Query, and Report. The date and time are shown as Apr 3, 2008 10:25:48 PM CDT. The user is logged in as Administrator (psadmin) with options for Logout and Activate. A 'Select Case' dropdown is set to 'No Case Selected...'. The main section is titled 'Query Event Data' and includes a 'Query type: Event Raw Messages ranked by Time, 0h:10m' with Edit and Clear buttons. A table below shows query criteria for Source IP, Destination IP, Service, Events, Device, Reported User, Keyword, Operation, Rule, and Action. The Keyword field is highlighted with a red box and contains the value 'NR-6936/0'. Below the table is a 'Specify raw message keywords:' section with a 'Search String' field containing 'NR-6936/0' and a 'Close' button. A table below the search string shows a list of keywords with 'None' selected for the Operation column. The interface includes 'Apply', 'Cancel', and 'Apply' buttons at the bottom.

Source IP	Destination IP	Service	Events	Device	Reported User	Keyword	Operation	Rule	Action
ANY	ANY	ANY	ANY	ANY	ANY	NR-6936/0	None	ANY	ANY

Search String	Close	Operation
NR-6936/0		None
		None
		None
		None
		None
		None
		None
		None
		None

The following screen shot shows the query results for these vulnerabilities created by the Cisco Security MARS appliance:

SUMMARY INCIDENTS **QUERY / REPORTS** RULES MANAGEMENT ADMIN HELP  
 Query Batch Query Report Apr 3, 2008 10:24:59 PM EDT  
 QUERY / REPORTS | CS-MARS Standalone: R4-MARS v4.3 Login: Administrator (padmin) :: Logout :: Activate  
 Select Case: No Case Selected... View Cases New Cases  
 Load Report as On-Demand Query with Filter  
 Select Group... Incident ID: [ ] Show  
 Select Report... Session ID: [ ] Show  
 Query Event Data  
 Click the cells below to change query criteria:  
 Query type: Event Raw Messages ranked by Time, 0h:10m Edit Clear  

Source IP	Destination IP	Service	Events	Device	Reported User	Keyword	Operation	Rule	Action
ANY	ANY	ANY	ANY	ANY	ANY	NR-6936/0	None	ANY	ANY

 Save As Report Save As Rule Submit  
 Query Results  

Event / Session / Incident ID	Event Type	Time	Reporting	Raw Message	Path / Mitigation	Tune
E:367448449, S:367448449	Cisco Unified Communications Disaster Recovery Framework Security Bypass and Command Execution Vulnerability			192.168.150.60/52019 --> 192.168.208.63/4040 TCP Cisco Unified Communications Disaster Recovery Framework Security Bypass and Command Execution Vulnerability , [REDACTED], Time:1207279455, Risk Rating:75, VLAN:0, Port List: 4040		False Positive Tuning
E:367448453, S:367448453	Cisco Unified Communications Disaster Recovery Framework Security Bypass and Command Execution Vulnerability					False Positive Tuning

 1 to 2 of 2 25 per page  
 Copyright © 2003–2007 Cisco Systems, Inc. All rights reserved. Summary :: Incidents :: Query / Reports :: Rules :: Management :: Admin :: Help

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. MARS will not include these events in inspection rules, thus 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 and instructions for configuring dynamic signature updates are available at 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 1.1	2008-April-04	Added Mitigation and Identification information for Cisco IPS and Cisco MARS
Revision 1.0	2008-APRIL-03	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 Security Center](#)
- [Transit Access Control Lists: Filtering at Your Edge](#)
- [Cisco IOS NetFlow - Home Page on Cisco.com](#)
- [Cisco IOS NetFlow White Papers](#)
- [Cisco Network Foundation Protection White Papers](#)
- [Cisco Network Foundation Protection Presentations](#)
- [Understanding Access Control List Logging](#)
- [Embedded Event Manager in a Security Context](#)
- [Identifying Incidents Using Firewall and IOS Router Syslog Events](#)
- [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](#)
- [Risk Rating and Threat Rating: Simplify IPS Policy Management](#)
- [Cisco Security Monitoring, Analysis, and Response System](#)

---

**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)

<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.](#)