

Cisco Applied Mitigation Bulletin: Identifying and Mitigating Exploitation of the Cisco Video Surveillance Authentication Vulnerabilities

<http://www.cisco.com/warp/public/707/cisco-amb-20070905-video.shtml>

Revision 1.2

Last Updated 2007 September 07 1645 UTC (GMT)

For Public Release 2007 September 05 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 Video Surveillance IP Gateway and Services Platform Authentication Vulnerabilities* and provides identification and mitigation techniques that administrators can deploy on Cisco network devices.

Vulnerability Characteristics

There are multiple vulnerabilities in Cisco Video Surveillance IP Gateway video encoders and decoders, Cisco Services Platforms and Cisco Integrated Services Platforms that may allow remote users to gain complete administrative control of vulnerable devices. These vulnerabilities are summarized in the following subsections:

IP Gateway Encoder / Decoder Telnet Authentication Vulnerability: This vulnerability can be exploited remotely without authentication and without user interaction. Successful exploitation of this vulnerability enables an attacker to gain interactive shell access with administrative privileges on vulnerable devices. An attacker with access to a vulnerable device may be able to alter or delete video streams processed by the device, or cause a denial of service potentially resulting in the loss of surveillance coverage. The attack vector for exploitation is through Telnet packets using TCP port 23. This vulnerability has been assigned CVE name CVE-2007-4747.

Services Platform / Integrated Services Platform Default Authentication Vulnerability: This vulnerability can be exploited remotely with authentication (using default credentials) and without user interaction. Successful exploitation of this vulnerability enables an attacker to gain interactive shell access with administrative privileges on vulnerable devices. An attacker with access to a vulnerable device may be able to alter or delete video streams processed by the device, or cause a denial of service potentially resulting in the loss of surveillance coverage. The attack vector for exploitation is through Telnet packets using TCP port 23. This vulnerability has been assigned CVE name CVE-2007-4746.

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-20070905-video.shtml>

Mitigation Technique Overview

Cisco devices provide several countermeasures for the Telnet/default authentication vulnerabilities. Administrators are advised to consider these protection methods to be general security best practices for infrastructure devices and the traffic that transits the network.

Cisco IOS Software can provide effective means of exploit prevention using transit access control lists (tACLs).

This protection mechanism filters and drops packets that are attempting to exploit the vulnerabilities described in this document.

Effective exploit prevention can also be provided by the Cisco ASA 5500 Series Adaptive Security Appliance, the Cisco PIX 500 Series Security Appliance, and the Firewall Services Module (FWSM) for Cisco Catalyst 6500 Series switches and Cisco 7600 Series routers using transit access control lists (tACLs).

This protection mechanism filters and drops packets that are attempting to exploit the vulnerabilities described in this document.

Effective use of Cisco Intrusion Prevention System (IPS) event actions provides visibility into and protection against attacks that attempt to exploit the IP Gateway Encoder / Decoder Telnet Authentication Vulnerability.

Cisco IOS NetFlow can provide visibility into these 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.

The Cisco Security Monitoring, Analysis, and Response System (Cisco Security MARS) appliance can

also provide visibility through queries and event reporting.

Risk Management

Organizations should 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 in Information Security Engagements](#) 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.

- [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

In an effort to protect vulnerable devices 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 should 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.

The tACL policy denies unauthorized Telnet packets on TCP port 23 sent to affected devices. In the following example, 192.168.1.0/24 is the network IP address space 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.

!
access-list 150 permit tcp host 192.168.100.1 192.168.1.0 0.0.0.255 eq telnet
!

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

!
access-list 150 deny tcp any 192.168.1.0 0.0.0.255 eq telnet
!

!--- 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 icmp unreachables**. ICMP unreachable rate limiting can be changed from the default using the global configuration command **ip icmp rate-limit unreachable interval-in-ms**.

Identification: Transit Access Control Lists

After the administrator applies the tACL to an interface, the **show ip access-lists** command will identify the number of Telnet packets on TCP port 23 that have been filtered. Administrators should investigate filtered packets to determine whether they are attempts to exploit these vulnerabilities. Example output for **show ip access-lists 150** follows:

```

router#show ip access-lists 150
Extended IP access list 150
 10 permit tcp host 192.168.100.1 192.168.1.0 0.0.0.255 eq telnet
 20 deny tcp any 192.168.1.0 0.0.0.255 eq telnet (75 matches)
 30 deny ip any any
router#

```

In the preceding example, access list *150* has dropped **75 Telnet** packets on **TCP port 23** for ACE sequence ID 20.

Identification: Access List Logging

The **log** or **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.

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. 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.

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 vulnerabilities described in this document. Administrators should investigate flows to determine whether they are attempts to exploit these vulnerabilities or whether they are legitimate traffic flows.

```
router#show ip cache flow
IP packet size distribution (130472380 total packets):
  1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
    .000 .971 .006 .000 .001 .003 .000 .002 .000 .005 .001 .000 .000 .000 .000

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

IP Flow Switching Cache, 4456704 bytes
  59 active, 65477 inactive, 1958209 added
  30218405 aged polls, 0 flow alloc failures
  Active flows timeout in 1 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 402056 bytes
  118 active, 16266 inactive, 3916423 added, 1958209 added to flow
  0 alloc failures, 0 force free
  1 chunk, 14 chunks added
  last clearing of statistics never
```

Protocol	Total Flows	Flows /Sec	Packets /Flow	Bytes /Pkt	Packets /Sec	Active(Sec) /Flow	Idle(Sec) /Flow
TCP-Telnet	3391	0.0	20	41	0.0	5.3	9.4
TCP-FTP	19	0.0	6	68	0.0	0.8	5.8
TCP-FTPD	1	0.0	1	44	0.0	0.0	16.8
TCP-WWW	1088912	0.2	115	53	34.3	11.2	4.0
TCP-SMTP	2	0.0	1	42	0.0	0.0	16.2
TCP-X	1	0.0	1	44	0.0	0.0	16.0
TCP-BGP	1	0.0	1	44	0.0	0.0	16.0
TCP-NNTP	2	0.0	3	52	0.0	0.6	9.3
TCP-other	333564	0.0	11	201	1.0	1.8	6.5

UDP-DNS	2544	0.0	1	71	0.0	0.4	15.5
UDP-NTP	200467	0.0	1	76	0.0	0.0	15.4
UDP-other	234249	0.0	2	280	0.1	0.0	15.4
ICMP	36156	0.0	5	58	0.0	25.8	10.4
IPINIP	4	0.0	1	88	0.0	0.0	15.4
GRE	22140	0.0	2	89	0.0	0.0	18.0
IP-other	27497	0.0	2	87	0.0	0.0	17.1
Total:	1948950	0.5	66	58	35.6	7.1	7.5

SrcIf	SrcIPAddress	DstIf	DstIPAddress	Pr	SrcP	DstP	Pkts
Gi0/0	192.168.60.155	Gi0/0	192.168.181.180	06	E4BD	7CFD	1
Gi0/0	192.168.185.237	Gi0/1	192.168.1.1	06	58D2	3435	1
Gi0/0	192.168.192.248	Gi0/1	192.168.1.1	06	1D11	0017	1
Gi0/0	192.168.126.36	Gi0/1	192.168.1.1	06	1283	AE20	1
Gi0/0	192.168.212.157	Gi0/0	192.168.84.135	06	467F	0017	1
Gi0/0	192.168.163.29	Gi0/1	192.168.1.1	06	5FD4	3AA9	1
Gi0/0	192.168.145.131	Gi0/1	192.168.1.1	06	5F02	0017	1
Gi0/0	192.168.9.213	Gi0/1	192.168.1.1	06	4B6A	B361	1
Gi0/0	192.168.234.166	Gi0/1	192.168.1.1	06	AEBE	B143	1
Gi0/0	192.168.255.157	Gi0/1	192.168.1.1	06	0372	01DB	1
Gi0/0	192.168.140.71	Gi0/1	192.168.1.1	06	7307	0128	1
Gi0/0	192.168.48.86	Gi0/0	192.168.120.201	06	773E	0017	1
Gi0/0	192.168.10.1	Gi0/0	192.168.227.191	06	F7E2	0017	1
Gi0/0	192.168.10.1	Gi0/1	192.168.1.1	06	37D0	DE10	1
Gi0/0	192.168.122.146	Gi0/1	192.168.1.1	06	9CA6	0017	1
Gi0/0	192.168.10.1	Gi0/0	192.168.239.242	06	FF16	0017	1
Gi0/0	192.168.130.170	Null	192.168.1.1	06	A793	C0E0	1
Gi0/0	192.168.100.159	Gi0/0	192.168.110.57	06	58D6	0017	1
Gi0/0	192.168.12.58	Gi0/1	192.168.1.1	06	540D	CE7C	1
Gi0/0	192.168.206.100	Null	192.168.1.1	06	7A99	22BE	1
Gi0/0	10.88.226.1	Gi0/1	192.168.206.5	11	007B	007B	1
Gi0/0	192.168.101.185	Gi0/1	192.168.1.1	06	CCDA	34BE	1
Gi0/0	192.168.10.1	Gi0/0	192.168.91.8	06	975D	E497	1
Gi0/0	172.18.104.132	Gi0/1	192.168.150.60	06	1A29	D7DA	2
Gi0/0	192.168.49.121	Gi0/1	192.168.1.1	06	DFC8	6DE9	1
Gi0/0	192.168.72.198	Gi0/0	192.168.121.106	06	42BA	0017	1
Gi0/0	192.168.177.185	Gi0/1	192.168.1.1	06	8528	0017	1
Gi0/0	192.168.132.131	Null	192.168.243.213	06	428D	5844	1
Gi0/0	192.168.56.77	Gi0/1	192.168.1.1	06	E7DD	51CF	1
Gi0/0	192.168.30.84	Gi0/0	192.168.19.107	06	634E	DBDF	1
Gi0/0	192.168.82.58	Gi0/0	192.168.17.237	06	4983	B1EF	1
Gi0/0	192.168.116.191	Gi0/0	192.168.220.63	06	5C74	499B	1
Gi0/0	192.168.11.33	Gi0/1	192.168.1.1	06	89E3	0017	1

router#

In the preceding example, there are multiple flows for **Telnet on TCP port 23 (hex value 0017)**. The packets in these flows may indicate an attempt to exploit the vulnerabilities described in this document. Administrators should compare these flows to baseline utilization for Telnet traffic sent on TCP port 23 and also investigate the flows to determine whether they are sourced from untrusted hosts or networks.

To view only the traffic flows for Telnet packets on TCP port 23 (hex value 0017), the command **show ip cache flow | include SrcIf|_06_.*0017** will display the related NetFlow records as shown here:

```
router#show ip cache flow | include SrcIf|_06_.*0017
```

SrcIf	SrcIPAddress	DstIf	DstIPAddress	Pr	SrcP	DstP	Pkts
Gi0/0	192.168.127.36	Gi0/0	192.168.1.109	06	AB7D	0017	1
Gi0/0	192.168.106.229	Gi0/1	192.168.1.1	06	B944	0017	1
Gi0/0	192.168.10.1	Gi0/0	192.168.1.199	06	DAE0	0017	1

```

Gi0/0      192.168.10.1      Gi0/0      192.168.1.159      06 DA62 0017      1
Gi0/0      192.168.112.242    Gi0/1      192.168.1.1        06 A6FC 0017      1
Gi0/0      192.168.10.1       Gi0/0      192.168.1.33       06 D1BF 0017      1
Gi0/0      192.168.39.103     Gi0/1      192.168.1.1        06 F88B 0017      1
Gi0/0      192.168.110.123    Gi0/1      192.168.1.1        06 B041 0017      1
Gi0/0      192.168.118.84     Gi0/0      192.168.1.128     06 B4A9 0017      1
Gi0/0      192.168.102.129    Gi0/1      192.168.1.1        06 A6F9 0017      1
Gi0/0      192.168.226.246    Gi0/0      192.168.121.57     06 BB94 0017      1
Gi0/0      192.168.242.248    Gi0/0      192.168.1.101     06 3526 0017      1
Gi0/0      192.168.10.1       Gi0/0      192.168.73.147     06 3616 0017      1
Gi0/0      192.168.34.200     Gi0/1      192.168.1.1        06 E872 0017      1
Gi0/0      192.168.162.60     Gi0/1      192.168.1.1        06 6AD7 0017      1
Gi0/0      192.168.103.38     Gi0/0      192.168.1.0        06 A81E 0017      1
Gi0/0      192.168.142.54     Gi0/0      192.168.1.174     06 477E 0017      1
Gi0/0      192.168.10.1       Gi0/1      192.168.1.1        06 C4BF 0017      1
Gi0/0      192.168.10.1       Gi0/1      192.168.1.1        06 C5F9 0017      1
Gi0/0      192.168.178.120    Gi0/0      192.168.1.42       06 7E0A 0017      1
Gi0/0      192.168.40.142     Gi0/0      192.168.1.28       06 E445 0017      1
Gi0/0      192.168.10.1       Gi0/0      192.168.1.180     06 FAA4 0017      1
Gi0/0      192.168.10.1       Gi0/1      192.168.1.1        06 FAF4 0017      1
Gi0/0      192.168.178.21     Gi0/1      192.168.1.1        06 4344 0017      1
Gi0/0      192.168.10.1       Gi0/0      192.168.166.175    06 A9AD 0017      1
router#

```

Cisco ASA, PIX, and FWSM Firewalls

Mitigation: Transit Access Control Lists

In an effort to protect vulnerable devices 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 should 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.

The tACL policy denies unauthorized Telnet packets on TCP port 23 sent to affected devices. In the following example, 192.168.1.0/24 is the network IP address space 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.
!
access-list Transit-ACL-Policy extended permit tcp host 192.168.100.1 192.168.1
255.255.255.0 eq telnet
!
!
!--- The following vulnerability-specific access control entries
!--- (ACEs) can aid in identification of attacks.

```

```

!
access-list Transit-ACL-Policy extended deny tcp any 192.168.1.0 255.255.255.0
!

!--- 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 interfaces 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 Telnet packets on TCP port 23 that have been filtered. Administrators should investigate filtered packets to determine whether they are attempts to exploit these vulnerabilities. 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
 192.168.1.0 255.255.255.0 eq telnet (hitcnt=44)
access-list Transit-ACL-Policy line 2 extended deny tcp any 192.168.1.0
 255.255.255.0 eq telnet (hitcnt=76)
access-list Transit-ACL-Policy line 3 extended deny ip any any (hitcnt=33)
firewall#

```

In the preceding example, the access list *Transit-ACL-Policy* has dropped **76 Telnet** packets on **TCP port 23** 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 regexp** command extracts syslog messages from the

logging buffer on the firewall. These messages provide additional information about denied packets that could indicate attempts to exploit the vulnerabilities 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
Aug 08 2007 06:07:46: %ASA-4-106023: Deny tcp src outside:192.168.208.63/46539
    dst inside:192.168.1.1/23 by access-group "Transit-ACL-Policy"
Aug 08 2007 06:07:49: %ASA-4-106023: Deny tcp src outside:192.168.208.63/46539
    dst inside:192.168.1.1/23 by access-group "Transit-ACL-Policy"
Aug 08 2007 06:07:55: %ASA-4-106023: Deny tcp src outside:192.168.208.63/46539
    dst inside:192.168.1.1/23 by access-group "Transit-ACL-Policy"
Aug 08 2007 06:08:07: %ASA-4-106023: Deny tcp src outside:192.168.208.63/46539
    dst inside:192.168.1.1/23 by access-group "Transit-ACL-Policy"
Aug 08 2007 06:12:21: %ASA-4-106023: Deny tcp src outside:192.168.208.63/58521
    dst inside:192.168.1.163/23 by access-group "Transit-ACL-Policy"
Aug 08 2007 06:12:21: %ASA-4-106023: Deny tcp src outside:192.168.208.63/24458
    dst inside:192.168.1.135/23 by access-group "Transit-ACL-Policy"
Aug 08 2007 06:12:21: %ASA-4-106023: Deny tcp src outside:192.168.208.63/1313
    dst inside:192.168.1.1/23 by access-group "Transit-ACL-Policy"
Aug 08 2007 06:12:21: %ASA-4-106023: Deny tcp src outside:192.168.208.63/1313
    dst inside:192.168.1.120/23 by access-group "Transit-ACL-Policy"
Aug 08 2007 06:12:21: %ASA-4-106023: Deny tcp src outside:192.168.208.63/64114
    dst inside:192.168.1.21/23 by access-group "Transit-ACL-Policy"
```

In the preceding example, the messages logged for the tACL *Transit-ACL-Policy* show **Telnet** packets on **TCP port 23** sent to the address block assigned to the network infrastructure.

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](#).

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 IP Gateway Encoder / Decoder Telnet Authentication Vulnerability described in this document. Starting with signature update S300 for sensors running Cisco IPS version 6.x or 5.x, the IP Gateway Encoder / Decoder Telnet Authentication Vulnerability described in this document can be detected by signature 5703/0 (Signature Name: Video Surveillance IP Gateway Encoder / Decoder Telnet Authentication Vulnerability). Signature 5703/0 is enabled by default, triggers a *High* severity event, has a signature fidelity rating (SFR) of 95, and is configured with a default event action of **produce-alert**. Signature 5703/0 fires when a telnet connection is established on TCP port 23 to a vulnerable device. Firing of this signature may indicate a potential exploit of the IP Gateway Encoder / Decoder Telnet Authentication 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 IP Gateway Encoder / Decoder Telnet Authentication Vulnerability described in this document.

The establishment of the three-way TCP handshake is required to exploit this vulnerability, which reduces the possibility of successful attacks using spoofed IP addresses as well as false positive events for signature 5703/0.

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 this vulnerability. Threat prevention is achieved through a default override that performs an event action of **deny-connection-inline** for triggered signatures with a *riskRatingValue* greater than 90. Additional information about the risk rating and the calculation of its value is available in [Cisco IPS Risk Rating Explained](#).

Cisco IPS 5.x sensors deployed in inline protection mode will need to have 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 the **deny-connection-inline** event action on sensors deployed in inline protection mode provides the most effective exploit prevention.

Identification: IPS Signature Events

Signature: 5703/0 - Video Surveillance IP Gateway Encoder/Decoder Telnet Authentication Vulnerability

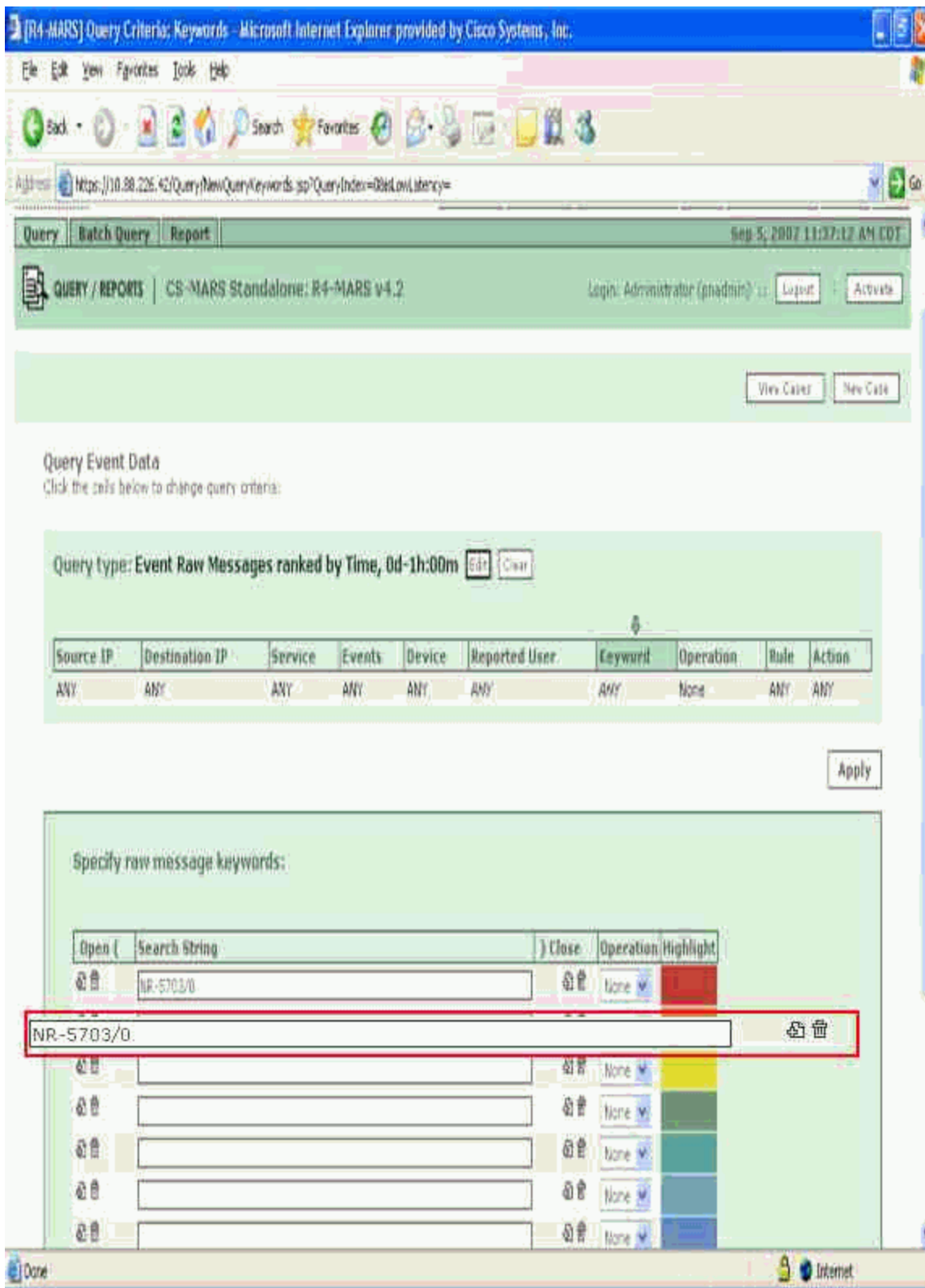
```
IPS# show events alert
evIdsAlert: eventId=1184079309278953323 severity=high vendor=Cisco
  originator:
    hostId: R4-IPS4240a
    appName: sensorApp
    appInstanceId: 6110
  time: 2007/09/05 13:28:04 2007/09/05 08:28:04 CDT
  signature: description=Video Surveillance IP Gateway Encoder/Decoder Telnet
             id=5703 version=S300
             subsigId: 0
             sigDetails: Video Surveillance IP Gateway Encoder/Decoder Telnet Authentica
             marsCategory: Info/SecPostureValidation/NoCredentials
  interfaceGroup: vs0
  vlan: 0
  participants:
    attacker:
      addr: locality=OUT 192.168.1.1
      port: 23
    target:
      addr: locality=OUT 10.94.165.10
      port: 40100
      os: idSource=learned relevance=relevant type=linux
  actions:
    denyPacketRequestedNotPerformed: true
    denyFlowRequestedNotPerformed: true
==== packet details removed ====
riskRatingValue: attackRelevanceRating=relevant targetValueRating=medium 90
threatRatingValue: 90
interface: ge0_0
protocol: tcp
```

Cisco Security Monitoring, Analysis, and Response System

Identification: Cisco Security Monitoring, Analysis, and Response System Query Type and Keyword

The Cisco Security Monitoring, Analysis, and Response System (Cisco Security MARS) appliance can query on events for the IP Gateway Encoder/Decoder Telnet Authentication Vulnerability using a query type and keyword. Using a keyword of **NR-5703/0** for IPS signature 5703/0, which was created for this vulnerability, and a query type of **All Matching Event Raw Messages** on the Cisco Security MARS appliance will provide a report that lists the events created by IPS signature 5703/0.

The following screen shot shows the values used to query for events created by IPS signature 5703/0 (Signature Name: Video Surveillance IP Gateway Encoder/Decoder Telnet Authentication Vulnerability).



The following screen shot shows the query results for NR-5703/0 created by the Cisco Security MARS appliance using a query type and keyword regex query.

[R4-MARS] Query Results - Microsoft Internet Explorer provided by Cisco Systems, Inc.

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites

Address: https://10.88.225.42/Query/QuerySubmit.js?ResultAndClearPaging=true&InlineReport=1

View Cases New Case

Load Report as On-Demand Query with Filter

Select Group: [v]
 Select Report: [v]

Incident ID: [] Show
 Session ID: [] Show

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

Query type: Event Raw Messages ranked by Time, 1d-0h [In] [Clear]

Source IP	Destination IP	Service	Events	Device	Reported User	Keyword	Operation	Rule	Action
ANY	ANY	ANY	ANY	ANY	ANY	NR-5703/D	None	ANY	ANY

Save As Report Save As Rule Submit

Query Results

Event / Session / Incident ID	Event Type	Time	Reporting Device	Raw Message	Path / Mitigation	Tune
E:254376065 S:254376065	Unknown Device Event Type [v]	Sep 5, 2007 8:20:04 AM CDT	R4-IP54140a	192.168.1.1/23 --> 10.94.165.10/40100 TCP Unknown Device Event Type [] Time:1188998884,Risk Rating:90,VLAN:0,Port List:40100,Action:cid:denyPacketRequestedNotPerformed cid:denyFlowRequestedNotPerformed	[] []	False Positive Tuning

192.168.1.1/23 --> 10.94.165.10/40100 TCP Unknown Device Event Type, []
 [] Time:1188998884,Risk Rating:90,VLAN:0,Port List:40100,Action:cid:denyPacketRequestedNotPerformed
 cid:denyFlowRequestedNotPerformed []

Copyright © 2007 Cisco Systems, Inc. All rights reserved.

Feedback

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 1.2	2007-September-07	Added CVE names to Vulnerability Characteristics section
Revision 1.1	2007-September-05	Added information for Cisco IPS and Cisco Security MARS
Revision 1.0	2007-September-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. 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](#)
- [Transit Access Control Lists: Filtering at Your Edge](#)
- [Understanding Access Control List Logging](#)
- [Cisco IOS NetFlow - Home Page on Cisco.com](#)
- [Cisco IOS NetFlow White Papers](#)
- [Cisco Network Foundation Protection White Papers](#)
- [Cisco Network Foundation Protection Presentations](#)
- [Cisco Firewall Products - Home Page on Cisco.com](#)
- [Cisco 6.x Intrusion Prevention System](#)
- [Cisco IPS Risk Rating Explained](#)
- [Cisco IPS 6.x Signature Downloads](#) ([registered](#) customers only)
- [Cisco IPS Signatures by Release Version](#) ([registered](#) customers only)
- [Cisco IPS Signatures by Signature ID](#) ([registered](#) customers only)
- [Cisco Security Monitoring, Analysis, and Response System](#)
- [Common Vulnerabilities and Exposures \(CVE\)](#) 

Help us help you.



Please rate this document.

- Excellent
- Good
- Average
- Fair
- Poor

This document solved my problem.

- Yes
- No
- Just browsing

Suggestions for improvement:

(256 character limit)

Home	How to Buy	Login	Profile	Feedback	Site Map	Help
----------------------	----------------------------	-----------------------	-------------------------	--------------------------	--------------------------	----------------------

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

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