

Cisco Applied Mitigation Bulletin: Identifying and Mitigating Exploitation of the Multiple Vulnerabilities in the Cisco Wireless Control System

Document ID: 91285

<http://www.cisco.com/warp/public/707/cisco-amb-20070412-wcs.shtml>

Revision 1.1

Last Updated 2007 April 13 1400 UTC (GMT)

For Public Release 2007 April 12 1600 UTC (GMT)

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

[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 "Multiple Vulnerabilities in the Cisco Wireless Control System." It documents additional mitigations that can be deployed on Cisco devices within the network.

Vulnerability Characteristics

There are three vulnerabilities associated with this Applied Mitigation Bulletin and the corresponding PSIRT security advisory. These vulnerabilities may result in the ability to write arbitrary files to the Wireless Control System (WCS), elevate privileges on the WCS, or access network organization information without authentication. The three vulnerabilities are summarized here:

- **Fixed FTP Credentials for WCS Location Backup.** This vulnerability may be exploited remotely using authentication with fixed credentials. Exploitation can allow the attacker to write arbitrary files to the server that is hosting the WCS application. In some cases, this capability could be leveraged to alter system files and compromise the server. The attack vector is through TCP ports 20 and 21. This vulnerability is not designated by a CVE ID.
- **Account Group Privilege Escalation.** This vulnerability may be exploited remotely with authentication using valid credentials of any user with a valid user name and password. This vulnerability allows a user to change his or her account group membership. This privilege escalation could allow full control of the WCS and the wireless networks managed by the WCS. The attack vector is through TCP ports 80 and 443. This vulnerability is not designated by a CVE ID.

- **Information Disclosure to Unauthenticated Users.** This vulnerability may be exploited remotely with no authentication. Exploitation can allow the attacker to obtain information about the organization of the network, including access point locations. The attack vector is through TCP ports 80 and 443. This vulnerability is not designated by a CVE ID.

This document contains information to assist Cisco customers in identifying and mitigating attempts to exploit the vulnerabilities in the Cisco WCS described above. Information about vulnerable, unaffected, and fixed software is available in the PSIRT security advisory:

<http://www.cisco.com/warp/public/707/cisco-sa-20070412-wcs.shtml>.

Mitigation Technique Overview

Cisco devices provide several countermeasures for the vulnerabilities in the Cisco Wireless Control System. Many of these countermeasures should be considered general security best practices.

The most preventive control is provided by access control lists (ACLs) applied on Cisco IOS software, Cisco PIX Security Appliances, Cisco ASA Adaptive Security Appliances, and Cisco Firewall Services Module (FWSM) for Cisco Catalyst 6500 Series switches and Cisco 7600 Series routers.

Detective controls can also be performed using Cisco IOS NetFlow and access control lists on Cisco IOS devices, Cisco PIX Security Appliances, Cisco ASA Adaptive Security Appliances, and Cisco FWSM for Cisco Catalyst 6500 switches and Cisco 7600 routers, as well as through syslog messages and counter values displayed in the output from **show** commands.

Risk Management

Organizations should follow their standard risk mitigation process to determine the potential impact of these vulnerabilities. Documents that may be used to aid in the risk triage are available at [Risk Triage for Security Vulnerability Announcements](#) and [Risk Triage and Prototyping](#).

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 Devices](#)
- [Cisco IOS NetFlow](#)
- [Cisco ASA, PIX, and FWSM Firewalls](#)
- [Cisco Intrusion Prevention System](#)
- [Cisco Security Monitoring, Analysis, and Response System](#)

Cisco IOS Devices

Mitigation: Infrastructure Access Control Lists

In an effort to protect infrastructure devices and minimize the risk, impact, and effectiveness of direct infrastructure attacks, infrastructure access control lists (iACLs) should be deployed to perform policy enforcement of traffic sent to infrastructure equipment. The construction of an iACL is accomplished by explicitly permitting only authorized traffic sent to infrastructure devices in accordance with existing security policies and configurations. iACLs deployed on Cisco IOS routers should be applied to all interfaces (where a Layer 3 IP address is configured) in the ingress direction for maximum protection of infrastructure devices.

In the following example, the address 192.168.2.2 belongs to the Wireless Location Appliance (WLA) and the address 192.0.2.2 belongs to the WCS. The iACL policy permits FTP packets from the WLA to the WCS and denies all other FTP flows to the WCS. The iACL policy also permits HTTP traffic from a trusted subnet (for example 192.168.3.0/24) and denies other HTTP traffic.

Added access control entries (ACEs) should be implemented as part of an iACL policy that is used to filter traffic at network ingress points.

For more information on iACLs, refer to [Protecting Your Core: Infrastructure Protection Access Control Lists](#).

```
! -- Permit/Deny additional Layer 3 and Layer 4 traffic sent to the
!-- infrastructure address space in accordance with existing security
!-- policies and configurations.

!

!-- Allow FTP packets from known trusted hosts (WLA) to the WCS.

access-list 100 permit tcp host 192.168.2.2 gt 1023 host 192.0.2.2 eq ftp
access-list 100 permit tcp host 192.168.2.2 gt 1023 host 192.0.2.2 eq ftp-data

!   Allow HTTP packets from known trusted subnet to the WCS

access-list 100 permit tcp 192.168.3.0 0.0.0.255 gt 1023 host 192.0.2.2 eq http

!-- The following vulnerability-specific ACEs
!--aid in the identification of attacks.

access-list 100 deny tcp any host 192.0.2.2 eq ftp
access-list 100 deny tcp any host 192.0.2.2 eq ftp-data
access-list 100 deny tcp any host 192.0.2.2 eq http

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

access-list 100 deny ip any 192.0.2.0 0.0.0.255

!-- Permit/deny all other Layer 3 or Layer 4 traffic in accordance with
!-- existing security policies and configurations.

!

!-- Apply access list to interface in the inbound direction.

interface FastEthernet0/0
ip access-group 100 in
!
```

Identification: Infrastructure Access Control Lists

With an iACL, once the access list has been applied to an interface in the ingress direction, the **show access-list** command can be used to identify the number of FTP packets that are being filtered. Filtered packets should be investigated to determine whether they are attempts to exploit this vulnerability. Example output for **show access-list 100** follows. In this example, there were **5 FTP packets** and **3 HTTP packets** dropped by access list 100. This access list has been applied in the inbound direction on interface FastEthernet0/0.

```
router#show access-list 100
Extended IP access list 100
 10 permit tcp host 192.168.2.2 gt 1023 host 192.0.2.2 eq ftp
 20 permit tcp host 192.168.2.2 gt 1023 host 192.0.2.2 eq ftp-data
 30 permit tcp 192.168.3.0 0.0.0.255 gt 1023 host 192.0.2.2 eq http
 40 deny tcp any host 192.0.2.2 eq ftp (5 matches)
 50 deny tcp any host 192.0.2.2 eq ftp-data
 60 deny tcp any host 192.0.2.2 eq http (3 matches)
 70 deny ip any 192.0.2.0 0.0.0.255
router#
```

Cisco IOS NetFlow

Identification

Cisco IOS NetFlow can be configured on Cisco IOS routers and switches to aid in the identification of traffic flows that may be potential attempts to exploit the vulnerabilities described in this document. Packets should be investigated to determine whether they are attempts to exploit this vulnerability or legitimate traffic.

```
router#show ip cache flow
IP packet size distribution (128222696 total packets):
 1-32  64  96  128  160  192  224  256  288  320  352  384  416  448  480
 .009 .619 .037 .008 .008 .008 .005 .012 .000 .001 .004 .001 .002 .002 .007

 512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
 .001 .001 .188 .012 .065 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 4456704 bytes
 20 active, 65516 inactive, 64268350 added
 191788566 aged polls, 0 flow alloc failures
 Active flows timeout in 1 minutes
 Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 402056 bytes
 20 active, 16364 inactive, 3795862 added, 3795862 added to flow
 0 alloc failures, 0 force free
 1 chunk, 11 chunks 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    11404486   2.6        1     49    3.0      0.0     1.5
TCP-FTP       6777       0.0        8     53    0.0      6.0     7.7
TCP-FTPD      673        0.0        3294  889   0.5      53.4    0.5
TCP-WWW       166480    0.0        13    747   0.5      4.2     9.3
TCP-SMTP      12         0.0        1     47    0.0      0.0    10.5
TCP-X         731        0.0        1     40    0.0      0.0     1.4
TCP-BGP       13         0.0        1     46    0.0      0.0    10.3
TCP-NNTP      12         0.0        1     47    0.0      0.0     9.7
TCP-Frag      70399     0.0        1    688   0.0      0.0    22.7
TCP-other     49169783  11.4       2    264   24.1     0.1     1.4
UDP-DNS       971384    0.2        1     58    0.2      0.0    15.4
UDP-NTP       1179572   0.2        1     76    0.2      0.6    15.5
UDP-TFTP      10         0.0        2     57    0.0      6.6    18.6
```

UDP-other	1023814	0.2	1	163	0.4	0.3	16.7
ICMP	273311	0.0	8	47	0.5	13.0	20.9
IPv6INIP	15	0.0	1	1132	0.0	0.0	15.4
GRE	694	0.0	1	50	0.0	0.0	15.4
IP-other	2	0.0	2	20	0.0	0.1	15.7
Total:	64268168	14.9	1	252	29.8	0.1	2.3

SrcIf	SrcIPAddress	DstIf	DstIPAddress	Pr	SrcP	DstP	Pkts
Gi0/1	192.168.132.44	Gi0/0	10.89.245.149	11	007B	007B	1
Gi0/1	192.168.128.23	Gi0/0	10.88.226.1	11	007B	007B	1
Gi0/1	192.168.2.2	Gi0/0	192.0.2.2	11	03B1	0015	21
Gi0/1	192.168.2.2	Gi0/0	192.0.2.2	11	03B2	0014	6
Gi0/1	192.168.150.1	Gi0/0*	128.63.2.53	11	0401	0035	1
Gi0/1	192.168.150.1	Gi0/0	128.63.2.53	11	0401	0035	1
Gi0/1	192.168.15.11	Gi0/0	192.0.2.2	11	05C7	0015	11
Gi0/0	10.88.226.1	Gi0/1*	192.168.128.23	11	007B	007B	1
Gi0/1	192.168.160.9	Gi0/0	192.0.2.2	11	1811	0015	8
Gi0/0	10.88.226.1	Gi0/1	192.168.128.23	11	007B	007B	1
Gi0/1	192.168.132.44	Gi0/0*	64.101.128.56	11	E094	0035	2
Gi0/1	192.168.132.44	Gi0/0	64.101.128.56	11	E094	0035	2
Gi0/0	192.168.208.64	Null	192.168.208.255	11	0089	0089	3
Gi0/1	192.168.128.56	Gi0/0	192.0.2.2	06	B184	0050	2
Gi0/1	192.168.3.44	Gi0/0	192.0.2.2	06	A301	0050	2
Gi0/0	64.101.128.56	Gi0/1*	192.168.132.44	11	0035	E094	2
Gi0/0	64.101.128.56	Gi0/1	192.168.132.44	11	0035	E094	2

router#

In the preceding example, there are several flows of FTP packets on TCP port 21 (hex value 0015) and TCP port 20 (hex value 0014). This traffic is being sourced from IP addresses in the 192.168.x.x address block and destined for IP address 192.0.2.2, which is the WCS. These flows should be compared to baseline utilization for FTP traffic and should also be investigated to determine whether the flows are sourced from trusted hosts and networks. There are also two flows of HTTP packets on TCP port 80 (hex value 0050). This traffic is also being sourced from IP addresses in the 192.168.x.x address block and destined for IP address 192.0.2.2, which is the WCS. These flows should be compared to baseline utilization for HTTP and investigated to determine whether the flows are trusted.

Cisco ASA, PIX, and FWSM Firewalls

Mitigation: Transit Access Control Lists

In an effort to protect the network from edge traffic that enters the network at ingress access points or traffic that transits the network, transit access control lists (tACLs) should be deployed to perform policy enforcement for this traffic. The construction of a tACL is accomplished by explicitly permitting only authorized traffic to enter the network at ingress points or permitting authorized traffic to transit the network in accordance with existing security policies and configurations.

These access list statements may be deployed on a Cisco ASA, PIX, or FWSM firewall as part of a firewall policy that will protect devices deployed behind it, including the WCS. The following access list permits FTP traffic on TCP ports 20 and 21 from a known trusted host, the WLC (for example, 192.168.2.2) to a WCS (for example, 192.0.2.2) and filters all other FTP traffic destined for the WCS. This access list also permits HTTP traffic on TCP port 80 from a trusted subnet (for example 192.168.3.0/24) and filters all other HTTP traffic destined for the WCS.

Care should be taken to allow required traffic for routing and administrative access prior to denying all unauthorized traffic. Whenever possible, infrastructure address space should be distinct from the address space used for user and services segments. Using this addressing methodology will assist with the construction and deployment of tACLs.

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

```
!-- Permit FTP packets from the WLC to the WCS and filter other FTP traffic.

access-list outside extended permit tcp host 192.168.2.2 gt 1023
    host 192.0.2.2 eq ftp
access-list outside extended permit tcp host 192.168.2.2 gt 1023
    host 192.0.2.2 eq ftp-data
access-list outside extended permit tcp 192.168.3.0 0.0.0.255 gt 1023
    host 192.0.2.2 eq http
access-list outside extended deny tcp any host 192.0.2.2 eq ftp
access-list outside extended deny tcp any host 192.0.2.2 eq ftp-data
access-list outside extended deny tcp any host 192.0.2.2 eq http

!-- Permit/deny all other IP traffic in accordance
!-- with existing security policies and configuration.

!

!-- Apply access list to interface in the inbound direction.

access-group outside in interface outside
!
```

Identification: Transit Access Control Lists

When an access list has been applied to an interface on an ASA, PIX, or FWSM firewall, the **show access-list** command can be used to identify the number of packets being filtered. Filtered packets should be investigated to determine whether they are attempts to exploit this vulnerability. Example output for **show access-list outside** follows. In this example, there were **16 FTP packets** destined for the WCS on TCP port 21 and **5 HTTP packets** destined for the WCS on TCP port 80 and dropped by access list *outside*. This access list has been applied in the inbound direction on the outside interface.

```
ASA5520# show access-list outside
access-list outside; 6 elements
access-list outside line 1 extended permit tcp host 192.168.2.2 gt 1023
    host 192.0.2.2 eq ftp (hitcnt=0) 0x39e4b2b3
access-list outside line 2 extended permit tcp host 192.168.2.2 gt 1023
    host 192.0.2.2 eq ftp-data (hitcnt=0) 0x473839eb
access-list outside line 3 extended permit tcp 192.168.3.0 0.0.0.255
    host 192.0.2.2 eq http (hitcnt=0) 0xef3df216
access-list outside line 4 extended deny tcp any host 192.0.2.2 eq ftp
    (hitcnt=16) 0xaa1c10b3
access-list outside line 5 extended deny tcp any host 192.0.2.2 eq ftp-data
    (hitcnt=0) 0x3521deb5
access-list outside line 6 extended deny tcp any host 192.0.2.2 eq http
    (hitcnt=5) 0x441d98d1
```

Cisco Intrusion Prevention System

Identification

The Cisco Intrusion Prevention System (IPS) appliances and service modules can be used to provide threat detection and prevention for attempts to exploit the Account Group Privilege Escalation vulnerability described in this document.

Beginning with signature update S280, IPS signature 5851/0 (Signature Name: WCS Administrative Directory Access) will trigger a low-severity alarm on potential attempts to exploit the Account Group

Privilege Escalation vulnerability or the Information Disclosure to Unauthenticated Users vulnerability, which may indicate an attempt to gain control of the WCS. Because this signature triggers a low-severity event, customers may not see this event on the IPS monitoring consoles. The following low-severity event was triggered on a Cisco IPS Sensor deployed in promiscuous mode.

```
R4-IPS4240a#show events alert
```

```
evIdsAlert: eventId=1166761098236260780 severity=low vendor=Cisco
  originator:
    hostId: R4-IPS4240a
    appName: sensorApp
    appInstanceId: 380
  time: 2007/04/13 00:04:31 2007/04/12 19:04:31 CDT
  signature: description=WCS Administrative Directory Access id=5851 version=S280
    subsigId: 0
    sigDetails: WCS Administrative Directory Access
    marsCategory: Info/Misc/Web
    marsCategory: Penetrate/ViewFiles/HTTPSsource
  interfaceGroup: vs1
  vlan: 0
  participants:
    attacker:
      addr: locality=OUT 192.168.204.148
      port: 1871
    target:
      addr: locality=OUT 192.168.130.69
      port: 80
    os: idSource=unknown relevance=relevant type=unknown
  context:
    fromAttacker:
```

```
!-- Output suppressed
```

```
triggerPacket:
```

```
!-- Output suppressed
```

```
riskRatingValue: attackRelevanceRating=relevant targetValueRating=medium 37
threatRatingValue: 37
interface: ge0_1
protocol: tcp
```

Cisco Security Monitoring, Analysis, and Response System

Identification: CS MARS Keyword Query

The Cisco Security Monitoring, Analysis, and Response System (Cisco Security MARS) console can be monitored for attempts to exploit one of the vulnerabilities described in this document. The following query on the MARS appliance will display events triggered by signature 5851/0.

Note: This query has a Result Format containing *All Matching Event Raw Messages* and Keyword equal to *NR-5851/0*.

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

Address: https://10.88.226.42/Query/NewQueryKeywords.jsp?QueryIndex=0&LowLatency=

CISCO SYSTEMS

SUMMARY INCIDENTS **QUERY / REPORTS** RULES MANAGEMENT ADMIN HELP

Query Batch Query Report Apr 12, 2007 7:53:31 PM CDT

QUERY / REPORTS CS-MARS Standalone: R4-MARS v4.2 Login: Administrator (radmin) Logout Activate

View Cases New Cases

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

Query type: Event Raw Messages ranked by Time, Apr 12, 2007 6:00:00 PM CDT - Apr 12, 2007 7:10:00 PM CDT Edit Clear

Source IP	Destination IP	Service	Events	Device	Reported User	Keyword	Operation	Rule	Action
ANY	ANY	ANY	ANY	ANY	ANY	NR-5851/0	None	ANY	ANY

Apply

Specify raw message keywords:

Open (Search String) Close	Operation	Highlight
	NR-5851/0		None	
			None	
			None	
			None	
			None	
			None	
			None	
			None	
			None	

Cancel Apply

The following display is the result of the previous query for IPS events triggered by signature 5851/0:

Copyright © 2003, 2004 Cisco Systems, Inc. All rights reserved.

Summary :: Incidents :: Query / Reports :: Rules :: Management :: Admin :: Help :: [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 1.1	2007–April–13	Added device–specific information for Cisco Intrusion Prevention System and Cisco Security Monitoring, Analysis, and Response System.
Revision 1.0	2007–April–12	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

- [Infrastructure Protection Access Control Lists](#)
 - [Transit Access Control Lists](#)
-

All contents are Copyright © 2006–2007 Cisco Systems, Inc. All rights reserved. [Important Notices](#) and [Privacy Statement](#).

Updated: Apr 13, 2007

Document ID: 91285
