

Cisco Applied Mitigation Bulletin: Identifying and Mitigating Exploitation of the Default Password in Wireless Location Appliance

<http://www.cisco.com/warp/public/707/cisco-amb-20061013-wla.shtml>

Revision 1.0

For Public Release 2006 October 13 2300 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

This vulnerability can be exploited remotely with default authentication and no user interaction is necessary. An attacker who successfully exploits this vulnerability could take complete control of the Cisco 2700 Series Wireless Location Appliance (WLA). The attack vector is through the Secure Shell (SSH) protocol, using TCP/22. This vulnerability is not covered by a CVE ID.

This document contains information to assist Cisco customers in identifying and mitigating attempts to exploit the Default Password in Wireless Location Appliance (WLA) vulnerability. This vulnerability affects Cisco 2700 Series Wireless Location Appliance devices running software versions prior to 2.1.34.0. Vulnerable versions contain a default root username/password combination that allows SSH access to the device.

Note: This vulnerability still exists on upgraded installations unless explicit steps have been taken to change the password after the initial installation of the product.

Vulnerable, non-affected and fixed software information is available in the PSIRT Security Advisory at <http://www.cisco.com/warp/public/707/cisco-sa-20061012-wla.shtml>.

Mitigation Technique Overview

Cisco devices provide countermeasures for the Default Password in Wireless Location Appliance (WLA) vulnerability. Until a fixed version of software can be installed, the most effective means of exploit prevention is by changing the default root password to a non-trivial password. Exploitation of this vulnerability can also be mitigated by applying interface Access Control Lists (ACLs) to filter SSH (TCP/22) packets from all but known trusted source addresses that are destined for the WLA 2700 device itself. Since exploitation requires a valid TCP session, the risk of a spoofed IP address attack is minimized.

Device-Specific Mitigation and Identification

Specific information on mitigation and identification is available for these devices:

- [Internet Edge Routers](#)
- [Cisco ASA/PIX/FWSM Firewalls](#)
- [Cisco IOS Switches](#)
- [Cisco Intrusion Prevention System \(IPS\)](#)
- [Cisco Security MARS \(CS MARS\)](#)

Internet Edge Routers



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.

Mitigation

Interface Access Lists

The following access list permits SSH (TCP/22) packets from a trusted management network (i.e. 192.0.2.0/24) destined for the target WLA device (i.e. 192.168.131.100). All other SSH packets destined to the WLA device are dropped. Added access list entries should be implemented as part of a Transit Access Control List policy that filters transit and edge traffic at network ingress points.

For more information on ACLs, refer to [Transit Access Control Lists: Filtering at Your Edge](#).

```
!-- Allow the SSH (TCP/22) packets from known trusted source addresses  
!-- only to the destination WLA device (192.168.131.100).
```

```

access-list 100 permit tcp 192.0.2.0 0.0.0.255 host 192.168.131.100 eq 22

!-- Block SSH from all other source addresses.

access-list 100 deny tcp any host 192.168.131.100 eq 22

!-- 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
!
```

Identification

Interface Access Lists

With a transit access list, 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 attempts to exploit this vulnerability. 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 22 (282 matches)
 20 deny tcp any host 192.168.131.100 eq 22 (6 matches)
router-01#
```

In the above example, there were six (6) SSH 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 attempts are in progress to exploit this vulnerability.

Note: It should be acknowledged that the following provides valuable information when the WLA device is accessible via the Internet.

```

router-01#show ip cache flow
IP packet size distribution (81278239 total packets):
 1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
 .000 .088 .883 .013 .000 .000 .000 .006 .006 .000 .000 .000 .000 .000 .000
  512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000
```

```

IP Flow Switching Cache, 278544 bytes
 2 active, 4094 inactive, 1895463 added
13837182 aged polls, 0 flow alloc failures
Active flows timeout in 30 minutes
Inactive flows timeout in 15 seconds

```

```

IP Sub Flow Cache, 25736 bytes
 2 active, 1022 inactive, 1895463 added, 1895463 added to flow
 0 alloc failures, 180 force free
 1 chunk, 20 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	31	0.0	27	54	0.0	8.2	7.3
TCP-FTP	13	0.0	2	52	0.0	1.0	7.2
TCP-FTPD	11	0.0	1	49	0.0	0.0	8.0
TCP-WWW	83	0.0	1	56	0.0	0.0	14.5
TCP-SMTP	11	0.0	1	49	0.0	0.0	8.2
TCP-X	11	0.0	1	49	0.0	0.0	7.9
TCP-BGP	157408	0.0	1	40	0.0	0.0	1.5
TCP-NNTP	11	0.0	1	49	0.0	0.0	7.8
TCP-Frag	86	0.0	5837	120	0.1	13.6	15.4
TCP-other	1476953	0.3	6	72	2.2	0.8	2.3
UDP-NTP	44691	0.0	1	76	0.0	0.0	15.2
UDP-other	213550	0.0	330	78	16.4	18.9	15.4
ICMP	2602	0.0	55	127	0.0	0.6	15.4
Total:	1895461	0.4	42	77	18.9	2.7	4.0

```

router-01#

```

SrcIf	SrcIPaddress	DstIf	DstIPaddress	Pr	SrcP	DstP	Pkts
Fa0	10.86.216.66	Fa1	192.168.131.100	06	0a47	0016	66
Fa0	10.86.115.216	Fa1	192.168.131.100	06	14a2	0016	75
Fa0	10.86.20.216	Fa1	192.168.131.100	06	23b7	0016	92
Fa0	10.89.236.52	Fa1	192.168.131.100	06	1E19	0016	60
Fa0	10.89.236.78	Fa1	192.168.131.100	06	1D07	0016	33
Fa0	10.89.236.94	Fa1	192.168.131.100	06	1C2A	0016	27
Fa0	10.89.236.102	Fa1	192.168.131.100	06	1DD4	0016	95
Fa0	10.89.236.118	Fa1	192.168.131.100	06	1DA0	0016	74
Fa0	10.89.236.134	Fa1	192.168.131.100	06	1D4E	0016	121
Fa0	10.89.236.150	Fa1	192.168.131.100	06	1C0C	0016	39
Fa0	10.89.236.174	Fa1	192.168.131.100	06	1C04	0016	15
Fa0	10.89.236.190	Fa1	192.168.131.100	06	1D76	0016	78
Fa0	10.89.236.206	Fa1	192.168.131.100	06	1A6A	0016	82
Fa0	10.89.236.222	Fa1	192.168.131.100	06	1A03	0016	93
Fa0	10.89.236.230	Fa1	192.168.131.100	06	1B84	0016	45

In the above example, there are several SSH flows (DstP = Hex 0016) from non-trusted IP addresses destined to the WLA device (192.168.131.100) on TCP/22. This may indicate an attempt to exploit this vulnerability and should be compared to baseline utilization of these ports to the WLA device.

To only view SSH (TCP/22, Hex 0016) flows, the command **show ip cache flow | include SrcIf|0016** may be used as shown here:

```

router-01#show ip cache flow | include SrcIf|0016

```

SrcIf	SrcIPaddress	DstIf	DstIPaddress	Pr	SrcP	DstP	Pkts
Fa0	10.86.216.66	Fa1	192.168.131.100	06	0a39	0016	58
Fa0	10.86.216.66	Fa1	192.168.131.100	06	0a47	0016	66

Fa0	10.86.115.216	Fa1	192.168.131.100	06 14a2 0016	75
Fa0	10.86.20.216	Fa1	192.168.131.100	06 23b7 0016	92
Fa0	10.89.236.52	Fa1	192.168.131.100	06 1E19 0016	60
Fa0	10.89.236.78	Fa1	192.168.131.100	06 1D07 0016	33
Fa0	10.89.236.94	Fa1	192.168.131.100	06 1C2A 0016	27
Fa0	10.89.236.102	Fa1	192.168.131.100	06 1DD4 0016	95
Fa0	10.89.236.118	Fa1	192.168.131.100	06 1DA0 0016	74
Fa0	10.89.236.134	Fa1	192.168.131.100	06 1D4E 0016	121
Fa0	10.89.236.150	Fa1	192.168.131.100	06 1C0C 0016	39
Fa0	10.89.236.174	Fa1	192.168.131.100	06 1C04 0016	15
Fa0	10.89.236.190	Fa1	192.168.131.100	06 1D76 0016	78
Fa0	10.89.236.206	Fa1	192.168.131.100	06 1A6A 0016	82
Fa0	10.89.236.222	Fa1	192.168.131.100	06 1A03 0016	93
Fa0	10.89.236.230	Fa1	192.168.131.100	06 1B84 0016	45

router-01#

Cisco ASA/PIX/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 SSH (TCP/22) packets from trusted management networks destined to a WLA device or devices.

PIX/ASA 7.x

The following access list permits SSH (TCP/22) packets from the 192.0.2.0/24 trusted management network destined to the WLA device (i.e. 192.168.131.100). All other SSH packets destined to the WLA device are dropped.

```
!-- Allow the SSH (TCP/22) packets from known trusted source addresses
!-- only to the destination WLA device.
```

```
access-list SSH remark Allow trusted network to send SSH packets to the destina
access-list SSH extended permit tcp 192.0.2.0 255.255.255.0 host 192.168.131.10
```

```
!-- Block SSH from all other source addresses.
```

```
access-list SSH remark Deny all other SSH traffic to the network device
access-list SSH extended deny tcp any host 192.168.131.100 eq ssh
access-list SSH remark Permit/deny all other IP traffic in accordance
with existing security policies and configurations
```

```
!-- Apply SSH access list inbound to outside interface.
```

```
access-group SSH in interface outside
```

FWSM

The following access list permits SSH (TCP/22) packets from the 192.0.2.0/24 trusted management network destined to the WLA device (i.e. 192.168.131.100). All other SSH packets destined to the WLA device are dropped.

```
!-- Allow the SSH (TCP/22) packets from known trusted source addresses  
!-- only to the destination WLA device.
```

```
access-list SSH remark Allow trusted network to send SSH packets to the destina  
access-list SSH extended permit tcp 192.0.2.0 255.255.255.0 host 192.168.131.10
```

```
!-- Block SSH from all other source addresses.
```

```
access-list SSH remark Deny all other SSH traffic to the network device  
access-list SSH extended deny tcp any host 192.168.131.100 eq ssh  
access-list SSH remark Permit/deny all other IP traffic in accordance  
with existing security policies and configurations
```

```
!-- Apply SSH access list inbound to outside interface.
```

```
access-group SSH in interface outside
```

Identification

PIX/ASA 7.x

```
pix#show access-list SSH  
access-list SSH; 2 elements  
access-list SSH line 1 remark Allow trusted network to send SSH packets to the  
access-list SSH line 2 extended permit tcp 192.0.2.0 255.255.255.0 host 192.168  
access-list SSH line 3 remark Deny all other SSH traffic to the network device  
access-list SSH line 4 extended deny tcp any host 192.168.131.100 eq ssh (hitcn  
access-list SSH line 5 remark Permit/deny all other IP traffic in accordance  
with existing security policies and configurations  
pix#
```

In the above example, 100 SSH packets have been received from a non-trusted host or network and were blocked. In addition, the following syslog message will be sent for any attempts that are blocked by access list SSH:

```
Oct 3 2006 15:08:55: %PIX-4-106023: Deny tcp src outside:10.89.236.157/32782  
dst inside:192.168.131.100/22 by access-group "SSH"
```

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

FWSM

```
fws-01#show access-list SSH
```

```
access-list SSH; 2 elements
access-list SSH line 1 remark Allow trusted network to send SSH packets to the
access-list SSH line 2 extended permit tcp 192.0.2.0 255.255.255.0 host 192.168
access-list SSH line 3 remark Deny all other SSH traffic to the network device
access-list SSH line 4 extended deny tcp any host 192.168.131.100 eq ssh (hitcn
access-list SSH line 5 remark Permit/deny all other IP traffic in accordance
    with existing security policies and configurations
fws-01#
```

In the above example, 100 SSH packets have been received from a non-trusted host or network and were blocked. In addition, the following syslog message will be sent for any attempts that are blocked by access list SSH:

```
Oct 3 2006 14:13:36: %FWSM-4-106023: Deny tcp src outside:10.89.236.157/32952
dst inside:192.168.131.100/22 by access-group "SSH"
```

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 IOS Switches



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.

Mitigation

Interface Access Lists

The following access list permits TCP/22 (SSH) packets from a trusted management network (i.e. 192.0.2.0/24) destined for the target WLA device (i.e. 192.168.131.100). All other SSH packets are dropped. Added access list entries should be implemented as part of a Transit Access Control List that filters transit and edge traffic at network ingress points. For more information on ACLs, refer to [Transit Access Control Lists: Filtering at Your Edge](#).

```
!-- Allow the SSH (TCP/22) packets from known trusted source addresses
!-- only to the destination WLA device.
```

```
ip access-list extended SSH
    permit tcp 192.0.2.0 0.0.0.255 host 192.168.131.100 eq 22
```

```
!-- Block SSH from all other source addresses.
```

```
deny tcp any host 192.168.131.100 eq 22
```

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

```
!-- Apply access list to physical/logical interface in the inbound direction.
```

```
interface Vlan10
 ip address 192.168.9.103 255.255.255.0
 ip access-group SSH in
!
```

Identification: {Insert content here}

With a transit access list, once the interface access list is applied, the **show access-lists** command can be used to identify the number of packets being filtered. Filtered packets should be investigated to determine if they are attempts to exploit this vulnerability. Example output for **show access-lists SSH**:

```
cat6k-01#show access-lists SSH
Extended IP access list SSH
 10 permit tcp 192.0.2.0 0.0.0.255 host 192.168.131.100 eq 22
 20 deny tcp any host 192.168.131.100 eq 22 (15 matches)
 30 permit ip any any (361 matches)
cat6k-01#
```

In the above example, there were 15 SSH packets dropped by access list SSH, which is applied in the inbound direction on VLAN interface Vlan10.

Note: The above hit counts displayed are for those packets processed (dropped) in software. For hardware-based IOS switches, an additional command can be used to determine if packets are being dropped in hardware.

Starting with IOS version 12.2(14)SX (for Supervisor 720) and version 12.2(17d)SXB (for Supervisor 2), the command **show tcam interface vlan <vlan-id> acl <in/out> ip** can be used to provide ACE hit counts that have occurred in hardware.

```
cat6k-01#show tcam interface vlan 10 acl in ip
permit tcp 192.0.2.0 0.0.0.255 host 192.168.131.100 eq 22
punt ip any host 192.168.9.102
deny tcp any host 192.168.131.100 eq 22 (match)
permit ip any any fragments
permit ip any any (match)
deny ip any any
deny ip any any fragments
cat6k-01#
```

Cisco Intrusion Prevention System (IPS)

Mitigation

The Cisco Intrusion Prevention System (IPS) can potentially be used to provide identification and threat mitigation of multiple attempts to exploit the Wireless Location Appliance default root password vulnerability starting with Cisco IPS Signature Update S111.

Signature Update S111 (released August 27, 2004) added signature 3653/0, which detects rapid SSH connections from the same source to the same destination. Signature 3653/0 triggers when six (6) SSH connections are detected within a two (2) second interval.

In order to trigger preventative controls, the IPS signature 3653/0 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 this vulnerability will be TCP based and are unlikely to be spoofed.

Note: This signature detects rapid SSH connections usually associated with brute force attempts. An attacker that knows the root password could successfully exploit this vulnerability without triggering this signature. SSH is an encrypted protocol and detecting the username/password combination is not feasible.

Identification

Cisco IPS signature 3653/0 triggers a **Low** severity event upon detection of an attempt to potentially exploit the WLA default password vulnerability. An IPS 5.x device triggered the following event using signature 3653/0 after an exploit attempt of this vulnerability on the target victim at IP address 192.168.132.100.

```
sensor5x#show event alarm

evIdsAlert: eventId=1142678274372770078 severity=low
vendor=Cisco
originator:
  hostId: sensor5x
  appName: sensorApp
  appInstanceId: 339
time: 2006/10/10 20:33:47 2006/10/10 14:33:47 CST
signature: description=Multiple Rapid SSH Connections id=3653 version=S111
  subsigId: 0
  sigDetails: Multiple Rapid SSH Connections
interfaceGroup:
vlan: 0
participants:
  attacker:
    addr: locality=OUT 10.86.115.216
    port: 35266
  target:
    addr: locality=IN 192.168.132.100
    port: 22
context:
  fromTarget:
000000 53 53 48 2D 31 2E 39 39 2D 4F 70 65 6E 53 53 48 SSH-1.99-OpenSSH
000010 5F 33 2E 31 70 31 0A _3.1p1.
  fromAttacker:
000000 53 53 48 SSH
  riskRatingValue: 27
  interface: ge0_0
  protocol: tcp
sensor5x#
```

Note: Because of the "Low" severity setting of this signature, it may be necessary to modify the IDS/IPS event monitoring system in use to ensure that this particular event is reported.

Cisco Security MARS (CS MARS)

Identification

As depicted in the following examples, the CS MARS console can be monitored for attempts to exploit this vulnerability.

The first example shows the Event and Session information correlated to the attempted exploits of this vulnerability and the subsequent trigger of Signature 3653/0 on the IDS/IPS device. The "attacking" device is identified by IP address 10.86.115.216 and the target WLA device is identified by IP address 192.168.132.100.

Session Information

Session / Incident ID	Events	Source IP/Port	Destination IP/Port	Protocol	Time	Reporting Devices	Path / Mitigation	Tune
S:1108050066	Multiple Rapid SSH Connections Context data	10.86.115.216 3210	192.168.132.100 22	TCP	Oct 10, 2006 7:02:54 PM EDT	wall-ids4230-02		False Positive

Events Correlated to this Session

Event / Session / Incident ID	Event Type	Source IP/Port	Destination IP/Port	Protocol	Time	Reporting Device	Path / Mitigation	Tune
E:1108050066, S:1108050066	Multiple Rapid SSH Connections	10.86.115.216 3210	192.168.132.100 22	TCP	Oct 10, 2006 7:02:54 PM EDT	wall-ids4230-02		False Positive
E:1108050067, S:1108050066	Context data	10.86.115.216 3210	192.168.132.100 22	TCP	Oct 10, 2006 7:02:54 PM EDT	wall-ids4230-02		False Positive

1 to 2 of 2 25 per page

The following query on the CS MARS appliance will display events triggered by Signature 3653/0:

[MARS20-01] Query - Microsoft Internet Explorer provided by Cisco Systems, Inc.

Address: https://10.87.96.218/Query/index.jsp

Google

CISCO SYSTEMS

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

Query Batch Query Report Oct 11, 2006 1:17:58 PM EDT

QUERY / REPORTS | CS-MARS Standalone: MARS20-01 v4.2 Login: Administrator (pnadmin) :: Logout :: Activate

View Cases New Case

Load Report as On-Demand Query with Filter

All 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, 1d-0h Edit Clear

Source IP	Destination IP	Service	Events	Device	Reported User	Keyword	Operation	Rule	Action
ANY	ANY	ANY	ANY	wall-ids4230-02, IDSM2-rodh	ANY	3653/0	None	ANY	ANY

ANY Apply

Save As Report Save As Rule Submit Inline

Copyright © 2003, 2006 Cisco Systems, Inc. All rights reserved. Summary :: Incidents :: Query / Reports :: Rules :: Management :: Admin :: Help :: Feedback

Done Internet

The display in the following figure is the result of the previous query for IDS/IPS events triggered by Signature 3653/0:

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 1.0	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

- [IPS 5.x Signature Downloads](#) ([registered](#) customers only)
 - [Signatures by Release Version](#) ([registered](#) customers only)
 - [Cisco Intrusion Prevention System \(IPS\)](#)
 - [Cisco Security Monitoring, Analysis and Response System \(CS MARS\)](#)
 - [Cisco Systems IntelliShield Vulnerability Alert ID - 11875](#) (IntelliShield 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

[Home](#)

[How to Buy](#)

[Login](#)

[Profile](#)

[Feedback](#)

[Site Map](#)

[Help](#)