Cisco Wireless Control System の複数の脆弱性の識別し、軽減不正利用

Advisory ID: cisco-amb-20070412-wcs

http://tools.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20070412-wcs

リビジョン 1.1

一般公開 2007 年の 4 月に関しては 12 日 16:00 UTC（ GMT ）

目次

Cisco の対応

この適用対応策速報は、PSIRT セキュリティ アドバイザリ『Cisco Wireless Control System の複数の脆弱性』に関連するドキュメントです。 このドキュメントでは、ネットワーク内の Cisco のデバイス上で配備できる追加の緩和策について説明しています。

脆弱性の特性

この適用対応策速報に関連する 3 つの脆弱性と、それに対応する PSIRT セキュリティ アドバイザリがあります。 これらの脆弱性が悪用されると、Wireless Control System（ WCS ）への任意のファイルの書き込み、WCS での権限の昇格、ネットワーク組織情報への不正アクセスが可能になる場合があります。 これら 3 つの脆弱性を次にまとめます。

- **WCS ロケーション バックアップのための固定 FTP クレデンシャル：** この脆弱性は、固定クレデンシャルによる認証を使用して、リモートから悪用される可能性があります。 この脆弱性を悪用すると、攻撃者は WCS アプリケーションをホスティングしているサーバに任意のファイルを書き込むことができます。 場合によっては、システム ファイルを改ざんして、サーバに危害を及ぼすために、この機能が利用される可能性があります。 この攻撃方法は、TCP ポート 20 および 21 を介するものです。 この脆弱性には、CVE ID が割り当てられていません。
- **アカウント グループ権限の昇格：** この脆弱性は、有効なユーザ名とパスワードを持つ任意のユーザの有効なクレデンシャルを認証で使用することにより、リモートで悪用される可能性があります。 この脆弱性を悪用すると、ユーザはアカウント グループ メンバシップを変更できます。 この権限の昇格によって、WCS および WCS によって管理

されるワイヤレス ネットワークの完全な制御が可能になる場合があります。 この攻撃方法は、TCP ポート 80 および 443 を介するものです。 この脆弱性には、CVE ID が割り当てられていません。

- **認証されていないユーザへの情報漏えい**： この脆弱性は、認証なしで、リモートから悪用される可能性があります。 この脆弱性を悪用すると、攻撃者はネットワーク構成に関する情報（アクセス ポイントの場所など）を取得できます。 この攻撃方法は、TCP ポート 80 および 443 を介するものです。 この脆弱性には、CVE ID が割り当てられていません。

このドキュメントでは、上記の Cisco WCS の脆弱性を悪用しようとする攻撃を識別して影響を緩和するために Cisco のお客様を支援する情報を提供しています。 脆弱性のあるソフトウェア、該当しないソフトウェア、修正済みソフトウェアについては、次の PSIRT セキュリティ アドバイザリを参照してください。
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070412-wcs。

緩和テクニックの概要

Cisco デバイスには、Cisco Wireless Control System の脆弱性に対する複数の対応策が備わっています。 これらの対応策の多くは、一般的なセキュリティ ベスト プラクティスであると考えられます。

最も効果的な防止策は、Cisco IOS ソフトウェア、Cisco PIX セキュリティ アプライアンス、Cisco ASA 適応型セキュリティ アプライアンス、および Cisco Catalyst 6500 シリーズ スイッチと Cisco 7600 シリーズ ルータの Cisco Firewall Services Module（FWSM; ファイアウォール サービス モジュール）に Access Control List（ACL; アクセス コントロール リスト）を適用することです。

また、Cisco IOS デバイス、Cisco PIX セキュリティ アプライアンス、Cisco ASA 適応型セキュリティ アプライアンス、および Cisco Catalyst 6500 スイッチと Cisco 7600 ルータの Cisco FWSM 上の Cisco IOS NetFlow とアクセス コントロール リストに加え、syslog メッセージと **show** コマンドの出力に表示されるカウンタ値を確認することで攻撃を検出できます。

リスク管理

各組織はそれぞれの標準的リスク緩和プロセスに従ってこれらの脆弱性の潜在的な影響を判断する必要があります。 リスク トリアージを支援するために使用できるドキュメントは、『セキュリティ脆弱性アナウンスメントに対するリスク トリアージ』および『リスク トリアージとプロトタイピング』で提供されています。

デバイス特有の軽減および識別

注意： 緩和テクニックの効果は、製品の組み合せ、ネットワーク トポロジ、トラフィックの動作、組織のミッションなど、お客様の状況によって異なります。 設定を変更する際には、変更を適用する前にその設定の影響を評価する必要があります。

- Cisco IOS デバイス
- Cisco IOS NetFlow
- Cisco ASA、PIX、および FWSM ファイアウォール
- Cisco Intrusion Prevention System

- Cisco Security Monitoring, Analysis, and Response System

Cisco IOS デバイス

緩和策： インフラストラクチャ アクセス コントロール リスト

インフラストラクチャ デバイスを保護し、直接的なインフラストラクチャ攻撃によるリスクと影響を緩和するには、インフラストラクチャ アクセス コントロール リスト（iACL）を配備して、インフラストラクチャ機器に送信されたトラフィックに対してポリシーを適用する必要があります。 iACL の構築は、既存のセキュリティ ポリシーと設定に基づいて、許可されたインフラストラクチャ デバイス宛てのトラフィックのみを明示的に許可することによって達成されます。 インフラストラクチャ デバイスの保護を最大にするには、Cisco IOS ルータ上に配備された iACL を、入力方向で（レイヤ 3 IP アドレスが設定されている）すべてのインターフェイスに適用する必要があります。

次の例では、アドレス 192.168.2.2 が Wireless Location Appliance（WLA）に属し、アドレス 192.0.2.2 が WCS に属します。 この iACL ポリシーでは、WLA から WCS への FTP パケットが許可され、WCS へのその他のすべての FTP フローが拒否されます。 この iACL ポリシーでは、信頼できるサブネット（192.168.3.0/24 など）からの HTTP トラフィックの許可とその他の HTTP トラフィックの拒否も行われます。

追加された Access Control Entry（ACE; アクセス コントロール エントリ）は、ネットワーク入力ポイントでトラフィックをフィルタリングするために使用される、iACL ポリシーの一部として実装される必要があります。

iACLs に関する詳細については、コアを保護することを参照して下さい: インフラストラクチャ保護 ACL』を参照してください。

```
! -- 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 !
```

識別策： インフラストラクチャ アクセス コントロール リスト

iACL を使用する場合、入力方向でインターフェイスに iACL が適用されていると、**show access-list** コマンドを使用して、フィルタリングされている FTP パケットの数を確認できます。 フィルタリングされたパケットに対しては、この脆弱性を悪用しようとしていないかどうかを調査する必要があります。 次に **show access-list 100** の出力例を示します。 この例では、アクセス リスト 100 によって **5 個の FTP パケット**と **3 個の HTTP パケット**が廃棄されています。 このアクセス リストは、インターフェイス FastEthernet0/0 に入力方向で適用されています。

```
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

確認方法

Cisco IOS ルータおよびスイッチで Cisco IOS NetFlow を設定することにより、このドキュメントで説明されている脆弱性を悪用しようとしている可能性があるトラフィック フローを識別できます。 パケットを調べて、それらが脆弱性の悪用を試みたものか、または正規のトラフィックかを判別する必要があります。

```
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 ager 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#
```

前記の例では、TCP ポート 21（16 進数値 0015）および TCP ポート 20（16 進数値 0014）に FTP パケットのフローが複数あります。 このトラフィックは、192.168.x.x アドレス ブロック内の IP アドレスから送信され、IP アドレス 192.0.2.2（WCS のアドレス）に宛てられています。 これらのフローを FTP トラフィックのベースライン使用率と比較し、調査して、フローが信頼できないホストやネットワークから送信されたものかどうかを判定する必要があります。 また、TCP ポート 80（16 進数値 0050）にも HTTP パケットのフローが 2 つ存在します。 このトラフィックも、192.168.x.x アドレス ブロック内の IP アドレスから送信され、IP アドレス 192.0.2.2（WCS のアドレス）に宛てられています。 これらのフローを HTTP のベースライン使用率と比較し、調査して、これらのフローが信頼できるかどうかを判定する必要があります。

Cisco ASA、PIX、および FWSM ファイアウォール

緩和策： トランジット アクセス コントロール リスト

入力アクセス ポイントからネットワークに入るエッジ トラフィック、またはネットワークを通過するトラフィックからネットワークを保護するには、トランジット アクセス コントロール リスト（tACL）を配備して、トラフィックにポリシーを適用する必要があります。 tACL の構築は、既存のセキュリティ ポリシーと設定に基づいて、入力ポイントからネットワーク内に入ることを許可されたトラフィックのみを明示的に許可するか、ネットワークを通過することを許可されたトラフィックを許可することによって達成されます。

これらのアクセス リストの文は、WCS などのファイアウォールの背後に展開されたデバイスを保護するファイアウォール ポリシーの一部として、Cisco ASA、PIX、または FWSM ファイアウォールに配備される場合があります。 次のアクセス リストでは、既知の信頼できるホストである WLC（192.168.2.2 など）から WCS（192.0.2.2 など）への TCP ポート 20 および 21 の FTP トラフィックが許可され、WCS に宛てられた他のすべての FTP トラフィックがフィルタリングされます。 このアクセス リストでは、信頼できるサブネット（192.168.3.0/24 など）からの TCP ポート 80 の HTTP トラフィックの許可と、WCS に宛てられた他のすべての HTTP トラフィックのフィルタリングも行われます。

許可されないすべてのトラフィックを拒否する前に、ルーティングおよび管理アクセスに必要なトラフィックを許可するように注意する必要があります。 インフラストラクチャのアドレス レンジは、できるだけユーザおよびサービス セグメントに使用されるアドレス レンジとは別個にする

必要があります。 このようにアドレスを設定することで、tACL の構築と配備が容易になります。

tACL についての詳細は、『トランジット アクセス コントロール リスト： エッジでのフィルタリング』を参照してください。

```
!-- 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 !
```

識別策： トランジット アクセス コントロール リスト

アクセス リストが ASA、PIX、または FWSM ファイアウォールのインターフェイスに適用されていると、**show access-list** コマンドを使用して、フィルタリングされたパケットの数を確認できます。 フィルタリングされたパケットに対しては、この脆弱性を悪用しようとしていないかどうかを調査する必要があります。 次に **show access-list outside** の出力例を示します。 この例では、アクセス リスト *outside* によって、TCP ポート 21 で WCS に宛てられた **16 個の FTP パケット**と TCP ポート 80 で WCS に宛てられた **5 個の HTTP パケット**が廃棄されています。 このアクセス リストは、Outside インターフェイスに入力方向で適用されています。

```
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

確認方法

Cisco 侵入防御システム（IPS）アプライアンスおよびサービス モジュールを使用すると、このドキュメントで説明されているアカウント グループ権限の昇格の脆弱性を悪用しようとする攻撃に対する検出と防御ができます。

シグニチャアップデート S280 にはじまって、IPS シグニチャ 5851/0（シグニチャ名前: WCS 管理上のディレクトリ アクセスは）WCS の制御を得る試みを示すかもしれない非認証ユーザ脆弱性に取引グループ特権 拡大脆弱性か情報の漏えいを不正利用する潜在的な試みの下位重大度 アラームを誘発します。 このシグニチャは重大度「low」のイベントをトリガーするので、このイベ

ントは IPS 監視コンソールに表示されない場合があります。 次の重大度「low」のイベントは、無差別モードで配備された Cisco IPS センサーでトリガーされています。

```
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/HTTPSource
  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

識別策： CS MARS キーワード クエリー

Cisco Security Monitoring, Analysis, and Response System（Cisco Security MARS）コンソールで、このドキュメントで説明されている脆弱性のいずれかを悪用しようとする攻撃を監視できます。 MARS アプライアンス上で次のクエリーを実行すると、シグニチャ 5851/0 によってトリガーされたイベントが表示されます。

注: このクエリーでは、*All Matching Event Raw Messages* 結果形式と、キーワード *NR-5851/0* が使用されていることに注意してください。

次の表示は、シグニチャ 5851/0 によってトリガーされた IPS イベントに対する前のクエリーの結果です。

追加情報

本アドバイザリは無保証のものとしてご提供しており、いかなる種類の保証も示唆するものではありません。 本アドバイザリの情報およびリンクの使用に関する責任の一切はそれらの使用者にあるものとします。 また、シスコは本ドキュメントの内容を予告なしに変更したり、更新したりする権利を有します。

改訂履歴

リビジョン 1.1	2007 年 4 月 13 日	Cisco 侵入防御システムおよび Cisco Security Monitoring, Analysis, and Response System のデバイス別の情報を追加。
リビジョン 1.0	2007 年 4 月 12 日	初回公開リリース

Ciscoセキュリティ手順

セキュリティ上の問題の支援を得、Cisco からセキュリティ情報を受け取るために登録するシスコ製品のレポート セキュリティーの脆弱性の完全情報は http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html で Cisco Worldwide Web サイトで利用できます。 これには手順がのための押します Ciscoのセキュリティの告知に関する照会を含まれています。 すべての Cisco セキュリティ アドバイザリは、http://www.cisco.com/go/psirt から入手できます。

関連情報

- インフラストラクチャ保護 ACL
- トランジット アクセス コントロール リスト