Cisco Wireless Control System の SQL インジェクション脆弱性の識別し、軽減不正利用

Advisory ID: cisco-amb-20100811-wcs

http://tools.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20100811-wcs

リビジョン 1.0

一般公開 2010 年の 8 月に関しては 11 日 16:00 UTC（ GMT ）

目次

Cisco の対応

この応用軽減情報は *Cisco Wireless Control System* の PSIRT Security Advisory *SQL インジェクション脆弱性*ヘドキュメントガイド、管理者がネットワーク デバイスを on Cisco 配置できる識別および軽減手法を提供します。

脆弱性の特性

Cisco Wireless Control System （ WCS ）は SQL インジェクション脆弱性が含まれています。 この脆弱性は、認証を使用して、エンドユーザの操作を必要とせずに、リモートで悪用される可能性があります。 この脆弱性の正常な不正利用は攻撃者がデバイス構成を修正することを可能にするかもしれません; ユーザを作成し、修正し、削除して下さい; または WCS によって管理されるあらゆるワイヤレス デバイスの設定を修正して下さい。 不正利用のための不正侵入ベクトルは TCPポート 443 を使用して SSL パケットを通ってあります。

注: Cisco WCS のためのインストール プログラムがユーザが管理インターフェイスへのアクセスに使用するべきポート番号をカスタマイズすることを可能にするので選択された実際のポートを一致するために TCPポート 443 への参照は変更される必要があります。

この脆弱性は CVE 識別 CVE-2010-2826 を割り当てられました。

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-20100811-wcs。

緩和テクニックの概要

Ciscoデバイスはこの脆弱性に複数の対策を提供します。 これらの保護方法は、インフラストラクチャ デバイスとネットワークを通過するトラフィックのセキュリティを保護する一般的なベスト プラクティスであると考えられます。 資料のこのセクションはこれらの手法の外観を提供します。

Cisco IOS ® ソフトウェアはインフラストラクチャ アクセスコントロール アクセス· コントロール· リスト（iACLs）を使用してエクスプロイト防止の有効な手段（方法）を提供できます。 この保護 メカニズムはこの脆弱性を不正利用するように試みているパケットをフィルタリングし、廃棄します。

有効なエクスプロイト防止はまた Cisco ASA 5500 シリーズによって中継アクセスコントロール アクセス· コントロール· リスト（tACLs）を使用している Cisco Catalyst 6500 シリーズ スイッチおよび Cisco 7600 シリーズ ルータにおよび Firewall Services Module （FWSM）適応型セキュリティ アプライアンス（ASA）ソフトウェア提供することができます。 この保護 メカニズムはこの脆弱性を不正利用するように試みているパケットをフィルタリングし、廃棄します。

Cisco IOS NetFlow レコードはネットワークベース 不正利用試みに表示を提供できます。

Cisco IOS ソフトウェア、Cisco ASA、および FWSM ファイアウォールは **show コマンド**からの出力で表示される syslog メッセージおよびカウンタ値によって可視性を提供できます。

リスク管理

組織はこの脆弱性の潜在的影響を判別するために標準リスク評価および軽減プロセスに従うように助言されます。 トリアージとは、プロジェクトを分類して、成功する可能性が高い取り組みに優先順位を付けることです。 Cisco では、各組織の情報セキュリティ チームがリスクベースのトリアージを行う能力を身に着けるために役立つドキュメントを提供しています。 セキュリティーの脆弱性 お知らせのためのリスク トリアージはおよびリスク トリアージおよびプロトタイピング反復可能な機密 保護 評価および応答プロセスを開発するために組織を助けることができます。

デバイス特有の軽減および識別

注意： あらゆる軽減手法の効果は製品ミックス、ネットワーク· トポロジ、交通現象および組織代表団のような特定の顧客 状況によって決まります。 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。

ここでは緩和策と識別策に関する情報が次のデバイス別に提供されています。

- Cisco IOS ルータおよびスイッチ
- Cisco IOS NetFlow
- Cisco ASA および FWSM ファイアウォール

Cisco IOS ルータおよびスイッチ

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、リスクを、直接インフラストラクチャ不正侵入の影響最小限に抑えるためにおよび効果は、管理者 インフラストラクチャ 機器に送られるトラフィックのポリシー適用を行うために iACLs を展開するように助言されます。 iACL は、既存のセキュリ

ティ ポリシーと設定に基づいて、インフラストラクチャ デバイス宛ての正当なトラフィックのみを明示的に許可することによって構築されます。 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、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の入力方向で配備済みの iACL を適用する必要があります。 iACL 回避策はこの脆弱性に対して不正侵入が信頼されたソース ソース・ アドレスから起きるとき完全な保護を提供できません。

iACL ポリシーは影響を受けたデバイスに送信される TCPポート 443 の不正 な SSL パケットを拒否します。 次の例では、192.168.60.0/24 は影響を受けたデバイスによって使用する、192.168.100.1 のホストは影響を受けたデバイスへのアクセスを必要とする信頼されたソースとみなされます IP アドレス領域であり。 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、iACL の構築と配備が容易になります。

iACLs についての追加情報はコアの保護にあります: インフラストラクチャ保護 ACL』を参照してください。

```
 ip access-list extended Infrastructure-ACL-Policy
 ! !-- Include explicit permit statements for trusted sources !-- that require access on the
vulnerable port ! permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 443 ! !-- The
following vulnerability-specific access control entry !-- (ACE) can aid in identification of
attacks ! deny tcp any 192.168.60.0 0.0.0.255 eq 443 ! !-- Explicit deny ACE for traffic sent to
addresses configured within !-- the infrastructure address space ! deny ip any 192.168.60.0
0.0.0.255 ! !-- Permit or deny all other Layer 3 and Layer 4 traffic in accordance !-- with
existing security policies and configurations ! !-- Apply iACL to interfaces in the ingress
direction ! interface GigabitEthernet0/0 ip access-group Infrastructure-ACL-Policy in
```

インターフェイス アクセス リストを使用してフィルタリングを行うと、ICMP 到達不能メッセージが、フィルタリングされたトラフィックの送信元に返されるようになります。 これらのメッセージを生成すると、デバイスの CPU 使用率が上昇する可能性があります。 Cisco IOS ソフトウェアでの ICMP 到達不能メッセージの生成は、デフォルトで 500 ミリ秒につき 1 パケットまでに制限されています。 ICMP 到達不能メッセージの生成を無効にするには、インターフェイス コンフィギュレーション コマンド **no ip unreachables** を使用します。 ICMP 到達不能レート制限をデフォルト設定から変更するには、グローバル コンフィギュレーション コマンド **ip icmp rate-limit unreachable** *interval-in-ms* を使用します。

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

管理者がインターフェイスに iACL を加えた後、**show ip access-lists コマンドは** iACL が適用するインターフェイスでフィルタリングされた TCPポート 443 の SSL パケットの数を確認します。 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 ip access-lists Infrastructure-ACL-Policy** の出力例を示します。

```
router#show ip access-lists Infrastructure-ACL-Policy
Extended IP access list Infrastructure-ACL-Policy
    10 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 443
    20 deny tcp any 192.168.60.0 0.0.0.255 eq 443 (3713 matches)
    30 deny ip any 192.168.60.0 0.0.0.255
router#
```

前の例では、アクセス リスト インフラストラクチャ ACL *ポリシー*はアクセス・ コントロール・ リスト エントリ（ ACE ）ラインのための 20 **TCPポート 443 （ https ）の 3713 の SSL** パケット

を廃棄しました。

ACE カウンターおよび syslog イベントを使用して調査事件についての追加情報に関しては、ファイアウォールおよび IOS ルータ Syslog イベントによって加えられる知性 白書を使用して識別事件を参照して下さい。

管理者は特定の状態が満たされるとき見つかります組み込みイベント マネージャを ACE カウンターのような実装を提供するのに使用できます。 セキュリティ コンテキストの応用知性 白書によって組み込まれるイベント マネージャは方法についての追加詳細をこの機能を使用する提供します。

識別策： アクセス リスト ロギング

log および **log-input** アクセス コントロール リスト（ACL）オプションを使用すると、特定の ACE に一致するパケットがログに記録されます。 **log-input** オプションを使用すると、パケットの送信元および宛先の IP アドレスとポートに加え、入力インターフェイスのロギングが有効になります。

注意： アクセス コントロール リストのロギングは CPU に多大な負荷を与えることがあるので、使用する場合は細心の注意を払う必要があります。 ACL ロギングによる CPU への影響を左右する要素は、ログの生成、ログの送信、およびログが有効な ACE に一致するパケットを転送するプロセス交換です。

Cisco IOS ソフトウェアでは、**ip access-list logging interval** *interval-in-ms* コマンドを使用すると、ACL ロギングによって引き起こされるプロセス交換の影響を制限できます。 **logging rate-limit** *rate-per-second* [**except** *loglevel*] コマンドを使用すると、ログの生成と送信の影響を制限できます。

Supervisor Engine 720 または Supervisor Engine 32 を搭載した Cisco Catalyst 6500 シリーズ スイッチおよび Cisco 7600 シリーズ ルータでは、ACL ロギングによる CPU への影響をハードウェアで最適化することができます。

ACL ロギングの設定と使用についての詳細は、Applied Intelligence white paper『アクセス コントロール リストのログについて』を参照してください。

Cisco IOS NetFlow

識別策： NetFlow レコードを使用したトラフィック フローの識別

管理者はこの脆弱性を不正利用する試みであるかもしれないトラフィックフローの識別を援助するために Cisco IOS NetFlow IOS ルータおよびスイッチを on Cisco 設定できます。 管理者はこの脆弱性を不正利用する試みであるか、または正当 な トラフィックフローであるかどうか判別するためにフローを調査するために助言されます。

```
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 ager 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         192.168.10.203  Gi0/1         192.168.60.103  06 0986 01BB    37
Gi0/0         192.168.11.56   Gi0/1         192.168.60.178  06 0911 01BB    13
Gi0/1         192.168.150.60  Gi0/0         10.89.16.226    11 0016 01BB     1
Gi0/0         192.168.23.97   Gi0/1         192.168.60.18   06 0B3E 01BB     5
Gi0/0         192.168.12.12   Gi0/1         192.168.60.91   06 0B89 01BB     3
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  06 0BD7 01BB    11
Gi0/0         10.89.16.226    Gi0/1         192.168.150.60  06 12CA 0016     1
router#
```

前述の例では、**TCPポート 443（Hex 値 01BB）の SSL のための複数のフローがあります。**

TCPポート 443（Hex 値 01BB）の SSL パケットのためのトラフィックフローだけ表示するため、コマンド **show ip cache flow | SrcIf|_06_.*01BB を**表示しますここに示されているように関連 TCP NetFlow レコードを**含んで下さい**:

```
router#show ip cache flow | include SrcIf|_06_.*01BB
SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Gi0/0         192.168.10.203  Gi0/1         192.168.60.103  06 0986 01BB    37
Gi0/0         192.168.11.56   Gi0/1         192.168.60.178  06 0911 01BB    13
Gi0/0         192.168.23.97   Gi0/1         192.168.60.18   06 0B3E 01BB     5
Gi0/0         192.168.12.12   Gi0/1         192.168.60.91   06 0B89 01BB     3
Gi0/0         192.168.12.185  Gi0/1         192.168.60.239  06 0BD7 01BB    11
router#
```

Cisco ASA 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

インターネット接続ポイント、パートナーおよびサプライヤー接続ポイントを含むかもしれない

、入力アクセス ポイントでネットワークに入るネットワークまたは VPN 接続ポイントをトラフィックから保護するために、管理者はポリシー適用を行うために tACLs を展開するために助言されます。 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、入力アクセス 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。 tACL 回避策はこの脆弱性に対して不正侵入が信頼されたソース ソース· アドレスから起きるとき完全な保護を提供できません。

tACL ポリシーは影響を受けたデバイスに送信される TCPポート 443 の不正 な SSL パケットを拒否します。 次の例では、192.168.60.0/24 は影響を受けたデバイスによって使用する、192.168.100.1 のホストは影響を受けたデバイスへのアクセスを必要とする信頼されたソースとみなされます IP アドレス領域であり。 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。

tACLs についての追加情報は[アクセス コントロール リスト（ACL）送信中](#)です: エッジでのフィルタリング』を参照してください。

```
! !-- Include explicit permit statements for trusted sources !-- that require access on the
vulnerable port ! access-list tACL-Policy extended permit tcp host 192.168.100.1 192.168.60.0
255.255.255.0 eq 443 ! !-- The following vulnerability-specific access control entry !-- (ACEs)
can aid in identification of attacks ! access-list tACL-Policy extended deny tcp any
192.168.60.0 255.255.255.0 eq 443 ! !-- Permit or 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 tACL-Policy extended deny ip any any ! !-- Apply tACL to
interface(s) in the ingress direction ! access-group tACL-Policy 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

tACL がインターフェイスに加えられた後、管理者はずっとフィルタ処理されたである TCPポート 443 の SSL パケットの数を確認する **show access-list コマンドを**使用できます。 管理者はこの脆弱性を不正利用する試みであるかどうか判別するためにフィルタ処理されたパケットを調査するために助言されます。 **show access-list tACL ポリシー**のための出力例は続きます:

```
firewall#show access-list tACL-Policy
access-list tACL-Policy; 3 elements
access-list tACL-Policy line 1 extended permit tcp host 192.168.100.1
     192.168.60.0 255.255.255.0 eq https (hitcnt=3713)
access-list tACL-Policy line 2 extended deny tcp any
     192.168.60.0 255.255.255.0 eq https (hitcnt=221)
access-list tACL-Policy line 3 extended deny ip any any (hitcnt=8)
firewall#
```

前の例では、アクセス リスト tACL *ポリシー*は信頼できないホストかネットワークから届く **TCPポート 443（https）の 221 の SSL** パケットを廃棄しました。 また、syslog メッセージ *106023* には、送信元と宛先の IP アドレス、送信元と宛先のポート番号、拒否されたパケットの IP プロトコルなど、有益な情報が含まれている場合があります。

識別策： syslog

log キーワードを含まないアクセス コントロール エントリ（ACE）によって拒否されたパケットに対しては、ファイアウォール syslog メッセージ *106023* が生成されます。 この syslog メッセージについての追加情報は [Cisco ASA 5500 シリーズ システムログメッセージ](#)に、8.2 - 106023

あります。

Cisco ASA 5500 シリーズ用の Syslog の設定についての情報はモニタリングに-ロギングを設定すること適応型セキュリティ アプライアンス（ASA）ソフトウェアあります。 Cisco Catalyst 6500 シリーズ スイッチおよび Cisco 7600 シリーズ ルータのための FWSM の Syslog の設定についての情報は Firewall Services Module の監視にあります。

次の例では、**show logging | グレップ** *regex* コマンドはファイアウォールのロギング バッファから syslog メッセージを得ます。 これらのメッセージはこの資料に説明がある脆弱性を不正利用する潜在的な試みを示す可能性がある拒否されたパケットについての追加情報を提供します。 **grep** キーワードを付けて別の正規表現を使用すると、ログ メッセージに含まれる特定のデータを検索できます。

正規表現構文についての追加情報は正規表現の作成にあります。

```
firewall#show logging | grep 106023
  Aug 11 2010 00:15:13: %ASA-4-106023: Deny tcp src outside:192.0.2.18/2944
         dst inside:192.168.60.191/443 by access-group "tACL-Policy"
  Aug 11 2010 00:15:13: %ASA-4-106023: Deny tcp src outside:192.0.2.200/2945
         dst inside:192.168.60.33/443 by access-group "tACL-Policy"
  Aug 11 2010 00:15:13: %ASA-4-106023: Deny tcp src outside:192.0.2.99/2946
         dst inside:192.168.60.240/443 by access-group "tACL-Policy"
  Aug 11 2010 00:15:13: %ASA-4-106023: Deny tcp src outside:192.0.2.100/2947
         dst inside:192.168.60.115/443 by access-group "tACL-Policy"
  Aug 11 2010 00:15:13: %ASA-4-106023: Deny tcp src outside:192.0.2.88/2949
         dst inside:192.168.60.38/443 by access-group "tACL-Policy"
  Aug 11 2010 00:15:13: %ASA-4-106023: Deny tcp src outside:192.0.2.175/2950
         dst inside:192.168.60.250/443 by access-group "tACL-Policy"
firewall#
```

前の例では、tACL tACL *ポリシー*のために記録 される メッセージは影響を受けたデバイスに割り当てられるアドレスブロックに送信 される **TCPポート 443（https）**のための **SSL** パケットを示します。

ASA セキュリティ アプライアンスのための syslog メッセージについての追加情報は Cisco ASA 5500 シリーズ システムログメッセージに、8.2 あります。 FWSM のための syslog メッセージについての追加情報はシステムログメッセージを記録 する Catalyst 6500 シリーズ スイッチおよび Cisco 7600 シリーズ ルータ Firewall Services Module にあります。

syslog イベントを使用して調査事件についての追加情報に関しては、ファイアウォールおよび IOS ルータ Syslog イベントによって加えられる知性 白書を使用して識別事件を参照して下さい。

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 1.0	2010-August-11	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

- Cisco 適用対応策速報 (英語)
- Ciscoセキュリティ情報収集活動
- Ciscoセキュリティ IntelliShield アラート マネージャ サービス
- Cisco IOS NetFlow：Cisco.com のホーム ページ (英語)
- Cisco IOS NetFlow White Paper (英語)
- NetFlow パフォーマンス分析
- Cisco ファイアウォール製品：Cisco.com のホーム ページ (英語)
- Common Vulnerabilities and Exposures (CVE))