デフォルトの管理クレデンシャルが悪用される可能性

Informational

アドバイザリーID : cisco-sa-20070215-http
初公開日 : 2006-02-15 16:00
バージョン 1.0 : Final
回避策 : No Workarounds available
Cisco バグ ID :

日本語による情報は、英語による原文の非公式な翻訳であり、英語原文との間で内容の齟齬がある場合には、英語原文が優先します。

概要

これは、SymantecがWebサイト http://www.symantec.com/enterprise/security_response/weblog/2007/02/driveby_pharming_how_clicking_1.htmlおよびhttp://www.symantec.com/avcenter/reference/Driveby_Pharming.pdfに掲載した「Drive-by Pharming」というタイトルの研究論文を公開したことに対する回答です。特に、シスコの非消費者向け製品の一部に関連するSymantecのホワイトペーパーの情報に焦点を当てています。これらの製品は、次の「影響を受けるCiscoルータ」セクションで指定されています。

この対応の目的

このホワイトペーパーではシスコ製品の新しい脆弱性は明らかにされていないため、シスコはセキュリティアドバイザリではなく、この回答を発行しています。この対応の目的は、影響を受けるCiscoルータ（以下で確認）に事前設定されて出荷される可能性があるデフォルトのクレデンシャルを、初期設定時およびデバイスがパブリックネットワークに接続される前に変更する方法をお客様に通知することです。

影響を受けるCiscoルータ

Small Office/Home Office(SOHO)、Remote Office/Branch Office(ROBO)、およびテレワーカーのビジネスセグメント向けに販売されているシスコルータには、Cisco Router Web Setup Tool(CRWS)またはCisco Router and Security Device Manager(SDM)が含まれていることがあります。これらは、Cisco IOS用のWebベースのデバイス管理ツールです。ソフトウェアベースのルータ

これらのCiscoルータでは、CRWSまたはSDMがルータと通信できるように、Cisco IOS HTTPサーバがデフォルトで有効になっています。出荷時にCRWSまたはSDMがインストールされている場合、ルータの設定には、HTTP Webインターフェイス経由でルータにアクセスするために使用されるデフォルトのユーザ名とパスワードが設定されます。

次のCiscoルータの設定は、バージョン3.3.0ビルド31より前のCRWSの任意のバージョンに付属しているデフォルトのIOS設定に基づいていますが、デフォルトのユーザ名とパスワードが削除されていない場合、この攻撃方法の影響を受ける可能性があります。

- Cisco 806
- Cisco 826
- Cisco 827
- Cisco 827H
- Cisco 827-4v
- Cisco 828
- Cisco 831
- Cisco 836
- Cisco 837
- Cisco SOHO 71
- Cisco SOHO 76
- Cisco SOHO 77
- Cisco SOHO 77H
- Cisco SOHO 78
- Cisco SOHO 91
- Cisco SOHO 96
- Cisco SOHO 97

次のCiscoルータの設定は、バージョン2.3.3より前のSDMの任意のバージョンに付属するデフォルトのIOS設定に基づいていますが、デフォルトのユーザ名とパスワードが削除されていない場合、この攻撃方法の影響を受ける可能性があります。

出荷時にSDMのデフォルト設定が有効になっているユニットの詳細については、http://www.cisco.com/en/US/prod/collateral/routers/ps5318/product_data_sheet0900aecd800fd118.htmlにある表4「Ordering and Factory Shipping Options for Cisco SDM」を参照してください。

Cisco SDM対応ルータ	**Cisco SDM対応Cisco IOSリリース**
Cisco SB101 Cisco SB106 Cisco SB107	12.3(8)YG、12.4(2)T以降のリリース
Cisco 831	12.2(13)ZH以降のリリース 12.3(2)XA以降のリリース

Cisco 837	12.3(2)T以降のリリース 12.4(2)T以降のリリース
Cisco 836	12.2(13)ZH以降のリリース 12.3(2)XA以降のリリース 12.3(4)T以降のリリース 12.4(2)T以降のリリース
Cisco 851 Cisco 857	12.3(8)YI 12.4(2)T以降のリリース
Cisco 871 Cisco 876 Cisco 877 Cisco 878	12.3(8)YI 12.4(2)T以降のリリース
Cisco 1701	12.2(13)ZH以降のリリース 12.3(2)XA以降のリリース (Cisco SDMはCisco IOSリリース12.3(2)XFをサポートしていません)。 12.3(4)T以降のリリース 12.4(2)T以降のリリース
Cisco 1711 Cisco 1712	12.2(15)ZL以降のリリース 12.3(2)XA以降のリリース (Cisco SDMはCisco IOSリリース12.3(2)XFをサポートしていません)。 12.4(2)T以降のリリース
Cisco 1710 Cisco 1721 Cisco 1751 Cisco 1751-v Cisco 1760 Cisco 1760-v	12.2(13)ZH以降のリリース 12.3(2)XA以降のリリース (Cisco SDMはCisco IOSリリース12.3(2)XFをサポートしていません)。 12.2(13)T3以降のリリース 12.3(2)T以降のリリース 12.3(1)M以降のリリース 12.2(15)ZJ3（Cisco 1710またはCisco 1721では使用不可） 12.4(2)T以降のリリース
Cisco 1801 Cisco 1802 Cisco 1803 Cisco 1811	12.3(8)YI 12.4(2)T以降のリリース
Cisco 1812	12.3(8)YH以降のリリース 12.4(2)T以降のリリース

Cisco 1841	12.3(8)T4以降のリリース 12.4(2)T以降のリリース
Cisco 2610XM Cisco 2611XM Cisco 2620XM Cisco 2621XM Cisco 2650XM Cisco 2651XM Cisco 2691	12.2(11)T6以降のリリース 12.3(2)T以降のリリース 12.3(1)M以降のリリース 12.3(4)XD 12.2(15)ZJ3 12.4(2)T以降のリリース
Cisco 2801 Cisco 2811 Cisco 2821 Cisco 2851	12.3(8)T4以降のリリース 12.4(2)T以降のリリース
Cisco 3640 Cisco 3661 Cisco 3662	12.2(11)T6以降のリリース 12.2(11)T6以降のリリース 12.3(2)T以降のリリース 12.3(1)M以降のリリース 12.3(4)XD 12.2(15)ZJ3 12.4(2)T以降のリリース
Cisco 3620	12.2(11)T6以降のリリース 12.3(1)M以降のリリース
Cisco 3640A	12.2(13)T3以降のリリース 12.3(2)T以降のリリース 12.3(1)M以降のリリース 12.3(4)XD 12.2(15)ZJ3 12.4(2)T以降のリリース
Cisco 3725 Cisco 3745	12.2(11)T6以降のリリース 12.3(2)T以降のリリース 12.3(1)M以降のリリース 12.3(4)XD 12.2(15)ZJ3 12.4(2)T以降のリリース
Cisco 3825 Cisco 3845	12.3(11)T以降のリリース 12.4(2)T以降のリリース
Cisco 7204VXR	12.3(2)T以降のリリース 12.3(1)M以降のリリース

Cisco 7206VXR	12.4(2)T以降のリリース Cisco SDMは、Cisco 7000ルータのB、E、またはSトレインリリースをサポートしていません。
Cisco 7301	12.3(2)T以降のリリース 12.3(3)M以降のリリース 12.4(2)T以降のリリース Cisco SDMは、Cisco 7000ルータのB、E、またはSトレインリリースをサポートしていません。

IOS設定がCRWSまたはSDMアプリケーションとともに出荷されたデフォルトのIOS設定に基づいていない、上記のCiscoルータは、この攻撃方法の影響を受けません。

追加情報

Cisco IOS HTTPサーバは、CRWSやSDMなどのWebベースの設定ツールで使用するために、複数のCisco IOSデバイスでデフォルトで有効になっています。これらの製品がCRWSまたはSDMのいずれかを使用して設定されている場合、管理者がデバイスを初めて設定するときに、デフォルトの管理者クレデンシャルを変更するように求められます（以前のバージョンのCRWSでは、デフォルトのクレデンシャルの変更は要求されていません）。詳細については、https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20060712-crwsを参照してください)。

デバイスの初回設定がコマンドラインインターフェイス(CLI)を使用して行われ、Webベースのインターフェイスを使用していない場合、管理者はデフォルトのクレデンシャルを変更するように求められず、デバイス自体によって自動的に削除されることもありません。デフォルトのクレデンシャルを変更または削除しないと、Symantecの調査ペーパーで説明されているように、デバイスが悪用される可能性があります。

シスコは、Cisco Bug ID CSCse65910(登録ユーザ専用)を使用して新しいセキュリティ機能を導入しました。Cisco IOSではこの機能に対して、ユーザ名に新しいキーワード「one-time」を追加しています。デバイスに設定され、「ワンタイム」オプションを使用するユーザクレデンシャルは、ユーザが仮想端末(vty)回線またはコンソールポートを介してルータに接続する場合に一度だけ使用できます。Cisco IOSは、最初の使用後にこのクレデンシャルを実行コンフィギュレーションから削除します。デバイスの管理者は、次のコマンドを使用して、特権レベル15のユーザ名を追加する必要があります。

```
username "myuser" privilege 15 secret 0 "mypassword"
```

「myuser」と「mypassword」は、使用するユーザ名とパスワードに置き換え、スタートアップコンフィギュレーションへの変更を保存します。

SDMでは、SDMバージョン2.3.3以降のこのCisco IOS機能を利用します。この機能は、Cisco

Bug Toolkit（登録ユーザ専用）にCisco Bug ID CSCek35024(登録ユーザ専用)として記載されています。

シスコでは、これらのデバイスマネージャが初めて使用する際に使用するデフォルトのクレデンシャルを変更することをお勧めします。

推奨される回避策

Symantecのドキュメントに記載されている攻撃の種類に関連するリスクを軽減するために、デバイスに付属するデフォルトのクレデンシャル（ユーザ名とパスワードの組み合わせ）をすべて削除することをお勧めします。CiscoルータがSDMまたはCRWSによって設定または監視されておらず、ご使用の環境でIOS HTTPサーバが必要でない場合は、無効にする必要があります。

ネットワーク内のCiscoデバイスに適用可能な他の緩和策については、この応答に関連するCisco適用対応策速報(https://sec.cloudapps.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20070215-http)を参照してください。

- 回避策1:Cisco IOS HTTPサーバ機能の無効化
  CRWSまたはSDMデバイス管理ツールを使用せず、Cisco IOS HTTPサーバが提供する機能を必要としないお客様は、デバイス設定に次のコマンドを追加してCRWSまたはSDMを無効にすることができます。

```
no ip http server
no ip http secure-server
```

  デバイスにインストールされ実行されているCisco IOSバージョンがSSL機能をサポートしていない場合、2番目のコマンドはエラーメッセージを返す可能性があります。このエラーメッセージは無害であり、無視しても問題ありません。

- 回避策2：イネーブルパスワードの設定によるCisco IOS HTTPサーバへの要求の認証の有効化
  CRWSまたはSDMデバイス管理ツールを使用するお客様、またはCisco IOS HTTPサーバが提供する機能を必要とするお客様は、Cisco IOS HTTPサーバインターフェイスにアクセスするための認証メカニズムを設定する必要があります。1つのオプションは、イネーブルシークレットまたはイネーブルパスワードを設定することです。イネーブルパスワードは、他の方式が設定されていない場合にCisco IOS HTTPサーバによって使用されるデフォルトの認証メカニズムです。
  イネーブルシークレットパスワードを使用してhttpアクセスの認証を設定するには、デバイス設定に次のコマンドを追加します。

```
enable secret "mypassword"
ip http authentication enable
```

  「mypassword」を選択した強力なパスワードに置き換えます。強力なパスワードについては、サイトのセキュリティポリシーを参照してください。

http://www.cisco.com/en/US/tech/tk59/technologies_tech_note09186a00809d38a7.shtmlで入手できる『Cisco IOS Password Encryption Facts』というドキュメントでは、enable secretコマンドとenable passwordコマンドの違いについて説明しています。

- 回避策3：デフォルト以外の認証メカニズムを使用してCisco IOS HTTPサーバへの要求の認証を有効にする
  「回避策2」で説明されているデフォルトの方法を使用して認証を設定する代わりに、他のメカニズムを介してCisco IOS HTTPサーバにアクセスするための認証メカニズムを設定します。このような認証メカニズムには、ローカルユーザデータベースや、事前に定義されたAAA（認証、認可、アカウンティング）方式などがあります。
  Cisco IOS HTTPサーバの認証メカニズムを有効にする手順は、Cisco IOSのリリースやその他の要因によって異なるため、例は示しません。
  Cisco IOS HTTPサーバの認証メカニズムの設定方法に関する情報を必要とするお客様は、『AAA Control of the IOS HTTP Server』というドキュメント(http://www.cisco.com/en/US/tech/tk59/technologies_tech_note09186a008069bdc5.shtml)をお読みください。
  注：CRWSアプリケーションで使用するためにテストおよびサポートされる唯一の認証方式は、ローカルユーザデータベースです。その他の方法（外部RADIUSまたはTACACS+サーバの使用を含む）はサポートされていません。

参考資料

- ファーミングの定義
  「ソーシャルエンジニアリング[からの保護」からのファーミングの定義](#)を次に示します。
  「ファーミングは、ユーザーが正当なWebサイトにアクセスしようとするときに、偽のWebサイトにリダイレクトすることで、偽のWebサイトを利用します。このリダイレクトはドメインスプーフィングとも呼ばれ、ユーザーが特定のURLを入力するまでPC上で休止状態になっている電子メールのウイルスを介して、またはドメインネームシステム(DNS)ディレクトリをポイズニングすることによって実行できます。DNSは、Webアドレスと電子メールアドレスを数値文字列に変換します。ポイズドDNSでは、Webアドレスと数値文字列を関連付けるリンクが変更されるため、ユーザが特定のURLを入力すると誤ったWebサイトに誘導されます。偽のWebサイトに入力されたユーザ名やパスワードなどの安全な情報は、ハッカーによって捕捉されます。「」
  Â
- Cisco ルータにおけるセキュリティの向上
  ドキュメント『Improving Security on Cisco Routers』は、ネットワーク管理者がセキュリティを向上させるためにルータ（特に境界ルータ）の変更を検討すべきシスコの構成設定についての非公式なディスカッションです。

Â

シスコのセキュリティ手順

シスコ製品のセキュリティの脆弱性に関するレポート、セキュリティ障害に対する支援、およびシスコからのセキュリティ情報を受信するための登録に関するすべての情報は、シスコのワールドワイド ウェブサイト https://sec.cloudapps.cisco.com/security/center/resources/security_vulnerability_policy.html から入手できます。この情報には、シスコのセキュリティ通知に関して、報道機関が問い合せる場合の説明も含まれています。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。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070215-http

改訂履歴

バージョン	説明	セクション	日付
リビジョン 1.0	説明		日付

利用規約

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。