Cisco IOS SSL VPNの脆弱性

High

アドバイザリーID : cisco-sa-20100922-sslvpn
CVE-2010-2836
初公開日 : 2010-09-22 16:00
最終更新日 : 2012-09-21 19:17
バージョン 1.1 : Final
CVSSスコア : 7.8
回避策 : No Workarounds available
Cisco バグ ID : CSCtg21685

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

Cisco IOS®ソフトウェアには、Cisco IOS SSL VPN機能がHTTPリダイレクトを使用して設定されている場合に脆弱性が存在します。この脆弱性が不正利用されると、認証されていないリモートユーザが該当デバイスのメモリリークを引き起こし、その結果、デバイスのリロード、新しいTCP接続のサービス不能、その他のDenial of Service(DoS)状態を引き起こす可能性があります。

シスコはこの脆弱性に対処するソフトウェアアップデートをリリースしています。この脆弱性を軽減する回避策があります。

このアドバイザリは、https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100922-sslvpn で公開されています。

注：2010年9月22日のCisco IOSソフトウェアセキュリティアドバイザリバンドル公開には6件のCisco Security Advisoryが含まれています。5件のアドバイザリはCisco IOSソフトウェアの脆弱性に対処するもので、1件はCisco Unified Communications Managerの脆弱性に対処するものです。各アドバイザリには、そのアドバイザリで詳述された脆弱性を解決するリリースを記載しています。2010年9月22日およびそれ以前に公開されたすべてのCisco IOSソフトウェアの脆弱性を修正したリリースについては、次のURLにある表を参照してください。

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100922-bundle

個々の公開リンクは、次のリンクの「Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication」に掲載されています。

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep10.html

該当製品

脆弱性のある製品

該当するバージョンのCisco IOSソフトウェアを実行しているデバイスは、SSL VPNおよびHTTPポートリダイレクションが設定されている場合に脆弱性が存在します。

デバイスがCisco IOS SSL VPN用に設定されており、脆弱性が存在するかどうかを確認するには、次の方法を使用できます。

show running-config | include webvpnに「webvpn gateway <word>」が含まれている場合、デバイスはCisco IOS SSL VPN機能をサポートしています。「webvpn gateway」セクションの少なくとも1つにinserviceコマンドがあり、HTTPポートリダイレクションが設定されているデバイスは脆弱です。次の例は、Cisco IOS SSL VPNが設定された脆弱性のあるデバイスを示しています。

```
<#root>

Router#

show running | section webvpn

webvpn gateway Gateway
 ip address 10.1.1.1 port 443
 http-redirect port 80
 ssl trustpoint Gateway-TP
 inservice
 !
Router#
```

Cisco IOS SSL VPNをサポートするデバイスは、「webvpn gateway」が設定されていない場合は脆弱ではありません。

シスコ製品で稼働している Cisco IOS ソフトウェア リリースを確認するには、デバイスにログインして show version コマンドを使って、システム バナーを表示します。"Internetwork Operating System Software"、"Cisco IOS Software" あるいはこれらに類似するシステム バナーによってデバイスで Cisco IOS ソフトウェアが稼働していることを確認できます。 その後ろにイメージ名が括弧の間に表示され、続いて "Version" と Cisco IOS ソフトウエア リリース名が表示されます。他のシスコ デバイスでは、show version コマンドが存在しなかったり、別の出力が表示されたりします。

次の例は、シスコ製品でCisco IOSソフトウェアリリース12.4(20)Tが稼働し、インストールされているイメージ名がC2800NM-ADVSECURITYK9-Mであることを示しています。

```
<#root>
```

```
Router#

show version

Cisco IOS Software, 2800 Software (C2800NM-ADVSECURITYK9-M), Version 12.4(20)T, RELEASE SOFTWARE (fc
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2008 by Cisco Systems, Inc.
Compiled Thu 10-Jul-08 22:00 by prod_rel_team


! --- output truncated
```

Cisco IOSソフトウェアリリースの命名規則の追加情報は、次のリンクの「White Paper: Cisco IOS Reference Guide」で確認できます。http://www.cisco.com/warp/public/620/1.html

脆弱性を含んでいないことが確認された製品

次の製品は、この脆弱性の影響を受けません。

- Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス
- Cisco IOS XR ソフトウェア
- Cisco IOS XE ソフトウェア

他のシスコ製品において、このアドバイザリの影響を受けるものは現在確認されていません。

詳細

Cisco IOS SSL VPN機能は、インターネット上の任意の場所にいるユーザに企業サイトへのリモートアクセスを提供します。SSL VPNを使用すると、エンドユーザのデバイスにVPNクライアントソフトウェアをインストールしなくても、電子メールやWeb閲覧などの特定のエンタープライズアプリケーションに安全にアクセスできます。

Cisco IOS SSL VPNの詳細については、次のリンクの『Cisco IOS Software Release 12.4T SSL VPN feature guide』を参照してください。http://www.cisco.com/en/US/docs/ios/12_4t/12_4t11/htwebvpn.html

HTTPポートリダイレクションを使用してSSL VPN用に設定されたデバイスは、異常に接続解除されたSSLセッションの処理中にTransmission Control Block（TCB；伝送制御ブロック）をリークする可能性があります。不正利用が続くと、デバイスのメモリリソースが枯渇し、その結果、デバイスのリロード、新しいTCP接続のサービス不能、およびその他のDoS状態が発生する可能性があります。この脆弱性を不正利用するために認証は必要ありません。

この脆弱性を不正利用するには、完全なTCP 3ウェイハンドシェイクが必要です。メモリリークは、次の例に示すようにshow tcp briefコマンドを実行することで検出できます。

```
Router#

show tcp brief

TCB       Local Address      Foreign Address     (state)
468BBDC0  192.168.0.22.80   192.168.0.33.19794   CLOSEWAIT
482D4730  192.168.0.22.80   192.168.0.33.22092   CLOSEWAIT
482779A4  192.168.0.22.80   192.168.0.33.16978   CLOSEWAIT
4693DEBC  192.168.0.22.80   192.168.0.33.21580   CLOSEWAIT
482D3418  192.168.0.22.80   192.168.0.33.17244   CLOSEWAIT
482B8ACC  192.168.0.22.80   192.168.0.33.16564   CLOSEWAIT
46954EB0  192.168.0.22.80   192.168.0.33.19532   CLOSEWAIT
468BA9B8  192.168.0.22.80   192.168.0.33.15781   CLOSEWAIT
482908C4  192.168.0.22.80   192.168.0.33.19275   CLOSEWAIT
4829D66C  192.168.0.22.80   192.168.0.33.19314   CLOSEWAIT
468A2D94  192.168.0.22.80   192.168.0.33.14736   CLOSEWAIT
4688F590  192.168.0.22.80   192.168.0.33.18786   CLOSEWAIT
4693CBA4  192.168.0.22.80   192.168.0.33.12176   CLOSEWAIT
4829ABC4  192.168.0.22.80   192.168.0.33.39629   CLOSEWAIT
4691206C  192.168.0.22.80   192.168.0.33.17818   CLOSEWAIT
46868224  192.168.0.22.80   192.168.0.33.16774   CLOSEWAIT
4832BFAC  192.168.0.22.80   192.168.0.33.39883   CLOSEWAIT
482D10CC  192.168.0.22.80   192.168.0.33.13677   CLOSEWAIT
4829B120  192.168.0.22.80   192.168.0.33.20870   CLOSEWAIT
482862FC  192.168.0.22.80   192.168.0.33.17035   CLOSEWAIT
482EC13C  192.168.0.22.80   192.168.0.33.16053   CLOSEWAIT
482901D8  192.168.0.22.80   192.168.0.33.16200   CLOSEWAIT
```

上記の出力では、CLOSEWAIT状態のTransmission Control Block（TCB；伝送制御ブロック）は移行せず、メモリリークを示しています。上記の例でローカルアドレス192.168.0.22.80で示されているように、ローカルTCPポート80（HTTPの既知のポート）のTCP接続だけが関連することに注意してください。

この脆弱性は、Cisco Bug ID CSCtg21685(登録ユーザ専用)として文書化され、Common Vulnerabilities and Exposures(CVE)IDとしてCVE-2010-2836が割り当てられています。

回避策

この脆弱性の回避策として、SSL VPN接続のHTTPリダイレクションを無効にすることが可能です。SSL VPN接続のHTTPリダイレクションは、webvpn gatewayコンフィギュレーションモードでno http-redirect portコマンドを実行することによって無効になります。

また、clear tcp tcb *コマンドを使用して、ハングしたTCBを手動でクリアすると、TCBはCLOSED状態に移行します。しばらくすると、CLOSED状態がクリアされ、メモリが解放されます。

注：TCBをクリアすると、正当な接続とハングしている接続の両方がクリアされます。これには、デバイスへのリモート接続（Telnet接続やSSH接続など）も含まれます。

https://sec.cloudapps.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20090908-tcp24で入手できるCisco Applied Mitigation Bulletin(AMB)の「Identifying and Mitigating

Exploitation of the TCP State Manipulation Denial of Service Vulnerabilities in Multiple Cisco Products」には、ハングしたTCP接続の検出とクリアに使用できる2つの緩和策（EEMスクリプトとSNMP）が記載されています。

Embedded Event Manager(EEM)

脆弱性のあるCisco IOSデバイスでは、Tool Command Language(Tcl)に基づくCisco IOS Embedded Event Manager(EEM)ポリシーを使用して、この脆弱性によって引き起こされたハング、拡張、または無期限のTCP接続を識別して検出できます。このポリシーにより、管理者はCisco IOSデバイスのTCP接続を監視できます。Cisco IOS EEMがこの脆弱性の不正利用の可能性を検出すると、ポリシーはsyslogメッセージまたはSimple Network Management Protocol(SNMP)トラップを送信してTCP接続をクリアすることにより、応答をトリガーできます。このドキュメントで提供されているポリシーの例は、2つのコマンドの出力を定義された間隔で監視および解析し、監視しきい値が設定値に達したときにsyslogメッセージを生成し、TCP接続をリセットできるTclスクリプトに基づいています。

Tclスクリプトは、次のリンクの「Cisco Beyond: Embedded Event Manager (EEM) Scripting Community」からダウンロードできます。http://forums.cisco.com/eforum/servlet/EEM?page=eem&fn=script&scriptId=2041。次に、デバイスの設定例を示します。

```
!
    !-- Location where the Tcl script will be stored
    !

    event manager directory user policy disk0:/eem

!
    !-- Define variable and set the monitoring interval
    !-- as an integer (expressed in seconds)
    !

    event manager environment EEM_MONITOR_INTERVAL 60

!
    !-- Define variable and set the threshold value as
    !-- an integer for the number of retransmissions
    !-- that determine if the TCP connection is hung
    !-- (a recommended value to use is 15)
    !

    event manager environment EEM_MONITOR_THRESHOLD 15

!
    !-- Define variable and set the value to "yes" to
```

```
    !-- enable the clearing of hung TCP connections
    !


    event manager environment EEM_MONITOR_CLEAR yes


!
    !-- Define variable and set to the TCP connection
    !-- state or states that script will monitor, which
    !-- can be a single state or a space-separated list
    !-- of states
    !


    event manager environment EEM_MONITOR_STATES CLOSEWAIT


!
    !-- Register the script as a Cisco EEM policy
    !


    event manager policy monitor-sockets.tcl

    !
```

詳細については、このAMBの「ハングしたTCP接続の検出とクリアEEM」および「SNMPを使用したハングしたTCP接続の検出とクリアEEM」(https://sec.cloudapps.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20090908-tcp24)を参照してください。

修正済みソフトウェア

アップグレードを検討する場合は、http://www.cisco.com/go/psirt と後続のアドバイザリも参照して、問題の解決状況と完全なアップグレード ソリューションを確認してください。

いずれの場合も、アップグレードする機器に十分なメモリがあること、および現在のハードウェアとソフトウェアの構成が新しいリリースで引き続き適切にサポートされていることの確認を十分に行ってください。情報に不明な点がある場合は、Cisco Technical Assistance Center（TAC）または契約を結んでいるメンテナンス プロバイダーにお問い合せください。

次のCisco IOSソフトウェアテーブルの各行は、Cisco IOSソフトウェアトレインに対応しています。特定のトレインに脆弱性が存在する場合、修正を含む最も古いリリースが「このアドバイザリの最初の修正済みリリース」列に記載されます。「2010年9月のバンドル公開に含まれるすべてのアドバイザリに対する最初の修正済みリリース」の列には、Cisco IOSソフトウェアセキュリティアドバイザリバンドル公開で公開されたすべての脆弱性を修正する最初のリリースが記載されています。シスコでは、可能な限り最新のリリースにアップグレードすることを推奨しています。

メジャーリリース	修正済みリリースの入手可能性	
Affected 12.0-Based Releases	このアドバイザリの最初の修正リリース	2010年9月のバンドル公開に含まれるすべてのアドバイザリに対する最初の修正リリース
該当する 12.0 ベースのリリースはありません。		
Affected 12.1-Based Releases	このアドバイザリの最初の修正リリース	2010年9月のバンドル公開に含まれるすべてのアドバイザリに対する最初の修正リリース
該当する 12.1 ベースのリリースはありません。		
Affected 12.2-Based Releases	このアドバイザリの最初の修正リリース	2010年9月のバンドル公開に含まれるすべてのアドバイザリに対する最初の修正リリース
影響を受ける 12.2 ベースのリリースはありません。		
Affected 12.3-Based Releases	このアドバイザリの最初の修正リリース	2010年9月のバンドル公開に含まれるすべてのアドバイザリに対する最初の修正リリース
該当する 12.3 ベースのリリースはありません。		
Affected 12.4-Based	このアドバイザリの最初の修正リリース	2010年9月のバンドル公開に含まれるすべてのアドバイザリに対する最初の

Releases		修正リリース
12.4	脆弱性なし	12.4(25d)
12.4GC	脆弱性なし	12.4(24)GC2
12.4JA	脆弱性なし	脆弱性なし
12.4JDA	脆弱性なし	脆弱性なし
12.4JDC	脆弱性なし	脆弱性なし
12.4JDD	脆弱性なし	脆弱性なし
12.4JHA	脆弱性なし	脆弱性なし
12.4JHB	脆弱性なし	脆弱性なし
12.4JK	脆弱性なし	脆弱性なし
12.4JL	脆弱性なし	脆弱性なし
12.4JMA	脆弱性なし	脆弱性なし
12.4JMB	脆弱性なし	脆弱性なし
12.4JX	脆弱性なし	脆弱性なし
12.4JY	脆弱性なし	脆弱性なし

12.4MD	脆弱性なし	12.4(24)MD2
12.4MDA	脆弱性なし	12.4(22)MDA4 12.4(24)MDA1
12.4MR	脆弱性なし	脆弱性あり(最初の修正は12.4MRA)
1240万	脆弱性なし	12.4(20)MRA1
12.4SW	脆弱性なし	脆弱性あり（最初の修正は12.4T）
12.4T	12.4(15)T13より前のリリースには脆弱性はありません。最初の修正12.4(15)T14 12.4(20)T5より前のリリースには脆弱性はありません。最初の修正12.4(20)T6 12.4(24)T2より前のリリースには脆弱性はありません。最初の修正12.4(24)T4	12.4(15)T14 12.4(20)T6 12.4(24)T4
12.4XA	脆弱性なし	脆弱性あり(最初の修正は12.4T)
12.4XB	脆弱性なし	脆弱性あり(最初の修正は12.4T)

12.4XC	脆弱性なし	脆弱性あり(最初の修正は12.4T)
12.4XD	脆弱性なし	脆弱性あり(最初の修正は12.4T)
12.4XE	脆弱性なし	12.4(6)XE5より前のリリースには脆弱性があり、12.4(6)XE5以降のリリースには脆弱性はありません。最初の修正は12.4T
12.4XF	脆弱性なし	脆弱性あり(最初の修正は12.4T)
12.4XG	脆弱性なし	脆弱性あり(最初の修正は12.4T)
12.4XJ	脆弱性なし	脆弱性あり(最初の修正は12.4T)
12.4XK	脆弱性なし	脆弱性あり(最初の修正は12.4T)
12.4XL	脆弱性なし	脆弱性あり。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください
12.4XM	脆弱性なし	脆弱性あり(最初の修正は12.4T)

12.4XN	脆弱性なし	脆弱性あり。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください
12.4XP	脆弱性なし	脆弱性あり。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください
12.4XQ	脆弱性なし	12.4(15)XQ6（2010年9月22日に入手可能）
12.4XR	脆弱性なし	12.4(15)XR9 12.4(22)XR7
12.4XT	脆弱性なし	脆弱性あり(最初の修正は12.4T)
12.4XV	脆弱性なし	脆弱性あり。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください
12.4XW	脆弱性なし	脆弱性あり(最初の修正は12.4T)
12.4XY	脆弱性なし	脆弱性あり(最初の修正は12.4T)

12.4XZ	脆弱性なし	脆弱性あり(最初の修正は12.4T)
12.4YA	脆弱性なし	脆弱性あり(最初の修正は12.4T)
12.4YB	脆弱性なし	脆弱性あり。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください
12.4YD	脆弱性なし	脆弱性あり。このアドバイザリの「修正済みソフトウェアの取得」セクションの手順に従って、サポート組織にお問い合わせください
12.4YE	脆弱性なし	12.4(24)YE1
12.4YG	脆弱性なし	12.4(24)YG3
影響を受ける 15.0 ベースのリリース	このアドバイザリの最初の修正リリース	2010年9月のバンドル公開に含まれるすべてのアドバイザリに対する最初の修正リリース
15.0M	15.0(1)M3	15.0(1)M3
15.0秒	Cisco 7600および10000シリーズルータ：脆弱性なし	Cisco 7600および10000シリーズルータ ：15.0(1)S1（2010年10月上旬に提供開始）

	Cisco IOS XE ソフトウェアの可用性を参照してください。	Cisco IOS XE ソフトウェアの可用性を参照してください。
15.0XA	脆弱性なし	脆弱性あり(最初の修正は15.1T)
15.0XO	脆弱性なし	脆弱性なし
影響を受ける 15.1 ベースのリリース	このアドバイザリの最初の修正リリース	2010年9月のバンドル公開に含まれるすべてのアドバイザリに対する最初の修正リリース
15.1T	15.1(1)T1 15.1(2)T0a	15.1(2)T1
15.1XB	脆弱性は15.1(1)XB1に制限されています。	脆弱性あり(最初の修正は15.1T)

Cisco IOS XE ソフトウェア

Cisco IOS XEリリース	このアドバイザリの最初の修正リリース	2010年9月のバンドル公開に含まれるすべてのアドバイザリに対する最初の修正リリース
2.1.x	脆弱性なし	脆弱性なし
2.2.x	脆弱性なし	脆弱性なし

2.3.x	脆弱性なし	脆弱性なし
2.4.x	脆弱性なし	脆弱性なし
2.5.x	脆弱性なし	脆弱性あり、2.6.2以降に移行
2.6.x	脆弱性なし	2.6.2
3.1.xS	脆弱性なし	脆弱性なし

Cisco IOS XEソフトウェアとCisco IOSソフトウェアリリースのマッピングについては、『Cisco IOS XE 2』および『Cisco IOS XE 3Sリリースノート』を参照してください。

Cisco IOS XRシステムソフトウェア

Cisco IOS XRソフトウェアは、2010年9月22日のCisco IOS Software Security Advisoryバンドル公開に含まれている脆弱性の影響を受けません。

推奨事項

$propertyAndFields.get("recommendations")

不正利用事例と公式発表

Cisco PSIRT では、本アドバイザリに記載されている脆弱性の不正利用事例やその公表は確認しておりません。

この脆弱性は、カスタマーサービスリクエストのトラブルシューティング中に発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100922-sslvpn

改訂履歴

リビジョン 1.0	2010年9月22日	初回公開リリース

利用規約

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。
本アドバイザリの記述内容に関して情報配信の URL を省略し、単独の転載や意訳を施した場合、当社が管理した情報とは見なされません。そうした情報は、事実誤認を引き起こしたり、重要な情報が欠落していたりする可能性があります。 このドキュメントの情報は、シスコ製品のエンドユーザを対象としています。

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。