Cisco IOSソフトウェアのSSL VPNにおけるDoS脆弱性

アドバイザリーID : cisco-sa-20140326-ios-sslvpn
CVE-2014-2112
初公開日 : 2014-03-26 16:00
バージョン 1.0 : Final
CVSSスコア : 7.8
回避策 : No Workarounds available
Cisco バグ ID : CSCuf51357

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ソフトウェアのセキュアソケットレイヤ(SSL)VPNサブシステムの脆弱性により、認証されていないリモートの攻撃者がサービス妨害(DoS)状態を引き起こす可能性があります。

この脆弱性は、特定のタイプのHTTP要求の処理に失敗することに起因します。この脆弱性を不正利用するために、攻撃者は、該当デバイスに対してメモリを消費するように巧妙に細工された要求を送信する可能性があります。この不正利用により、攻撃者は該当デバイスのメモリを消費し、断片化させる可能性があります。これにより、パフォーマンスの低下、特定のプロセスの障害、または影響を受けるデバイスの再起動が発生する可能性があります。

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はありません。

このアドバイザリは、次のリンクより確認できます。
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140326-ios-sslvpn

注： 2014年3月26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。すべてのアドバイザリは、Cisco IOSソフトウェアの脆弱性に対処しています。各Cisco IOSソフトウェアセキュリティアドバイザリには、このアドバイザリで詳述された脆弱性を修正したCisco IOSソフトウェアリリースと、2014年3月のバンドル公開のすべてのCisco IOSソフトウェアの脆弱性を修正したCisco IOSソフトウェアリリースが記載されています。

個々の公開リンクは、次のリンクにある『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_mar14.html

該当製品

脆弱性のある製品

WebVPN拡張機能(Cisco IOS SSLVPN)が設定されているデバイスのみが、この脆弱性の影響を受けます。

デバイスでWebVPNが有効になっているかどうかは、 show webvpn gateway EXECコマンドを発行することで確認できます。デバイスで脆弱なソフトウェアが実行されていて、設定で設定されているゲートウェイの Adminステータスと Operationステータスが upとリストされている場合は、そのデバイスに該当します。

次の例では、デバイスに ssl-vpnという名前の単一WebVPNゲートウェイが設定されています。ゲートウェイが起動し、接続を受け入れている

```
Router#show webvpn gateway

Gateway Name                        Admin  Operation
------------                        -----  ---------
ssl-vpn                             up     up
```

管理者は、EXECコマンド show running-config | include webvpnを発行します。デバイスから何らかの出力が返された場合は、そのデバイスにSSLVPNが設定されており、そのデバイスに脆弱性が存在する可能性があることを意味しています。 show running-config | include webvpnには webvpn gateway <word>が含まれており、この場合は、デバイスがCisco IOS SSLVPN機能をサポートするように設定されています。 webvpn gatewayセクションの1つ以上に inserviceコマンドが設定されているデバイスは脆弱です。次の例は、Cisco IOS SSLVPNが設定された脆弱性のあるデバイスを示しています。

```
Router# show running-config | include webvpn

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

WebVPNゲートウェイが設定されていない場合、またはすべての設定済みWebVPNゲートウェイエントリのwebvpnゲートウェイセクションに no inserviceサブコマンドが含まれている場合、Cisco IOS SSLVPNをサポートするデバイス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、Cisco IOS ソフトウェア リリースが 15.2(4)M5、インストールされたイメージ名が C3900-UNIVERSALK9-M であるシスコ製品を示しています。

```
<#root>

Router>

show version

Cisco IOS Software, C3900 Software (C3900-UNIVERSALK9-M), 15.2(4)M5, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2013 by Cisco Systems, Inc.
Compiled Fri 13-Sep-13 16:44 by prod_rel_team



!--- output truncated
```

Cisco IOSソフトウェアのリリース命名規則の追加情報は、『White Paper: Cisco IOS and NX-OS Software Reference Guide』で確認できます。

脆弱性を含んでいないことが確認された製品

Cisco IOS XEソフトウェアは、この脆弱性の影響を受けません。

Cisco IOS XRソフトウェアは、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は、この脆弱性には該当しません。

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のDoS脆弱性

Cisco IOSソフトウェアのセキュアソケットレイヤ(SSL)VPNサブシステムの脆弱性により、認証

されていないリモートの攻撃者がサービス妨害(DoS)状態を引き起こす可能性があります。

この脆弱性は、特定のタイプのHTTP要求の処理に失敗することに起因します。この脆弱性を不正利用するために、攻撃者は、該当デバイスに対してメモリを消費するように巧妙に細工された要求を送信する可能性があります。この不正利用により、攻撃者は該当デバイスのメモリを消費し、断片化させる可能性があります。これにより、パフォーマンスの低下、特定のプロセスの障害、または影響を受けるデバイスの再起動が発生する可能性があります。
該当するデバイスへの悪意のある接続ごとに、3ウェイTCPハンドシェイクを完了する必要があります。ただし、認証は必要ありません。SSLVPNのデフォルトTCPポート番号は443です。
この脆弱性は、Cisco Bug ID CSCuf51357(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-2014-2112が割り当てられています。

回避策

このCiscoセキュリティアドバイザリに記載されている脆弱性に対する回避策はありません。

修正済みソフトウェア

ソフトウェアのアップグレードを検討する場合は、 http://www.cisco.com/go/psirt のシスコ セキュリティ アドバイザリ、応答、および通知のアーカイブや、後続のアドバイザリを参照して侵害の可能性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デバイス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規リリースで引き続き正しくサポートされていることを十分に確認してください。不明な点については、Cisco Technical Assistance Center（TAC）もしくは契約しているメンテナンスプロバイダーにお問い合わせください。

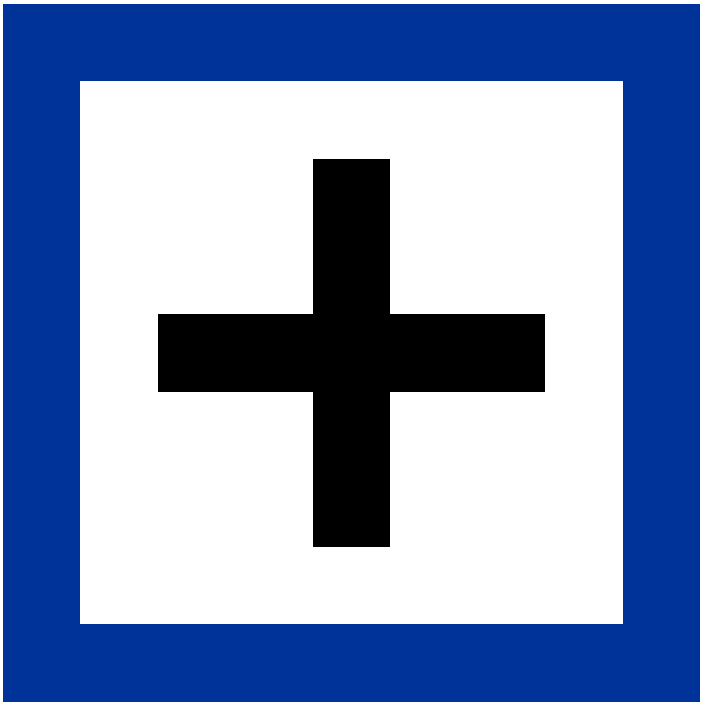
2014年2月、シスコは2005年から2010年の間に製造されたメモリコンポーネントに関する業界全体の問題の詳細を発表しました。これらのコンポーネントを使用するシスコ製品の大多数では、フィールドでの故障発生率が予想レベルを下回っていますが、デバイスのリロードや電源の再投入を行うと、コンポーネントの障害が発生する可能性があります。この問題に関連する既知のセキュリティ上の影響はありませんが、該当製品のサブセットでは、ソフトウェアアップグレードプロセス中にメモリコンポーネントの障害が発生する可能性があります。アップグレードを決定する前に、関連情報と製品固有のField Notice(www.cisco.com/go/memory)を確認することを推奨します。各Field Noticeには、ソフトウェアのアップグレード中に製品にメモリコンポーネントの障害が発生するかどうかが記載されています。

Cisco IOS ソフトウェア

Cisco IOSソフトウェアチェッカーは、Cisco IOSソフトウェアの脆弱性による侵害を最も迅速に判定する方法です。 このツールを使用すると、特定のCisco IOSソフトウェアリリースに影響を与えるシスコセキュリティアドバイザリをすばやく特定できます。 ドロップダウンメニューから

リリースを選択するか、ローカルシステムからファイルをアップロードすることで、検索を開始できます。このツールには、show versionコマンド出力の解析機能もあります。以前に公開されたすべてのシスコセキュリティアドバイザリ、特定の資料、または2014年3月のバンドル資料のすべてのアドバイザリを検索することで、結果をカスタマイズできます。

また、次のCisco IOSソフトウェアの表を使用して、問題の発生の有無を確認することもできます。 各行はCisco IOSソフトウェアリリースに対応しています。特定のリリースに脆弱性が存在する場合、その修正を含む最初のリリースが2列目に表示されます。3列目には、この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のすべての脆弱性を修正する最初のリリースを記載します。



展開して修正済みソフトウェアの詳細情報を表示

Cisco IOS XE ソフトウェア

Cisco IOS XEソフトウェアは、2014年3月の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。

Cisco IOS XR ソフトウェア

Cisco IOS XRソフトウェアは、2014年3月の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 Product Security Incident Response Team（PSIRT）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を確認していません。

この脆弱性は、お客様のケースの調査中にCisco TACによって発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140326-ios-sslvpn

改訂履歴

リビジョン 1.0	2014年3月26日	初回公開リリース

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。