Multiple Vulnerabilities in Cisco ASA Software

Advisory ID: cisco-sa-20130410-asa

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130410-asa/

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。

Revision 1.1

Last Updated 2013 May 23 14:16 UTC (GMT)

For Public Release 2013 April 10 16:00 UTC (GMT)

目次

要約

Cisco ASA ソフトウェアは次の脆弱性の影響を受けます。

- IKE バージョン 1 における DoS 脆弱性
- 細工された URL における DoS 脆弱性
- 細工された証明書検証における DoS 脆弱性
- DNS インスペクションにおける DoS 脆弱性

これらの脆弱性はそれぞれ独立しています。1 つの脆弱性に影響を受けるリリースが、その他の脆弱性からも影響を受けるとは限りません。

これらの脆弱性の不正利用が成功した場合、該当デバイスでリロードが発生し、DoS（サービス拒否）状態になることがあります。

シスコはこれらの脆弱性に対応するための無償ソフトウェア アップデートを提供しています。これらの脆弱性の一部については、回避策があります。

このアドバイザリは、次のリンクで確認できます。

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130410-asa/

注： Cisco Catalyst 6500 シリーズ スイッチおよび Cisco 7600 シリーズ ルータ用の Cisco Firewall Services Module（FWSM）は、上記の脆弱性の一部の影響を受ける可能性があります。Cisco FWSM に該当する脆弱性に関しては別途 Cisco Security Advisory が公開されています。このアドバイザリは次のリンクに掲載されています。

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130410-fwsm/

該当製品

Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス用 Cisco ASA ソフトウェア、Cisco Catalyst 6500 シリーズ スイッチおよび Cisco 7600 シリーズ ルータ用の Cisco ASA Services Moduleと、Cisco ASA 1000V Cloud Firewall は複数の脆弱性の影響を受けます。影響を受ける Cisco ASA ソフトウェアのバージョンは、脆弱性によって異なります。影響を受けるバージョンの詳細については、このアドバイザリの「ソフトウェア バージョンおよび修正」セクションを参照してください。

Cisco PIX セキュリティ アプライアンスは、このセキュリティ アドバイザリで説明されている脆弱性の一部に該当する場合があります。Cisco PIX はソフトウェア メンテナンス終了となっています。Cisco PIX セキュリティ アプライアンスをご利用のお客様は、Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンスに移行することを推奨します。

脆弱性が認められる製品

IKE バージョン 1 における DoS 脆弱性

Cisco ASA ソフトウェアを実行しているデバイスは、IKE バージョン 1 が有効になっている場合に、この脆弱性の影響を受けます。 **crypto isakmp enable <インターフェイス名>** コマンド（Cisco ASA ソフトウェア 8.3.x 以前）または **crypto ikev1 enable <インターフェイス名>** コマンド（Cisco ASA ソフトウェア 8.4.x 以降）が設定されている場合、IKE バージョン 1 が有効になっています。

IKE バージョン 1 はデフォルトでは有効になっていません。

細工された URL における DoS 脆弱性

Cisco ASA ソフトウェアを実行しているデバイスは、ネットワーク アクセス制御に Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）を使用していて、かつネットワーク ユーザの認証に HTTP(S) リスニング ポートが有効になっている場合、この脆弱性の影響を受けます。 **aaa authentication listener** コマンドが設定されている場合、ネットワーク ユーザの認証に HTTP(S) リスニング ポートが有効になっています。

ネットワーク アクセス制御用の AAA とネットワーク ユーザ認証用の HTTP(S) リスニング ポートは、デフォルトでは有効になっていません。

細工された証明書検証における DoS 脆弱性

Cisco ASA ソフトウェアが、サードパーティ認証局または Cisco ASA ローカル認証局で認証されたトラストポイントを 1 つ以上有する場合、この脆弱性の影響を受けます。

認証されたトラストポイントがCisco ASA ソフトウェアに設定されているかを確認するには、**show crypto ca certificate** コマンドを使用して証明書が 1 つ以上のトラストポイントに関連付けられているか検証します。次の例は、「*test*」というトラストポイントに関連付けられた証明書を示しています。

```
ciscoasa# show crypto ca certificates
[...]
Status: Available
[...]
Associated Trustpoints: test
```

デジタル証明書認証はデフォルトでは有効になっていません。

DNS インスペクションにおける DoS 脆弱性

Cisco ASA ソフトウェアは、DNS インスペクションが有効になっている場合、この脆弱性の影響を受けます。

DNS インスペクションが有効になっているかを確認するには、**show service-policy | include dns** コマンドを使用します。次の例は、DNS インスペクションが有効になっている Cisco ASA ソフトウェアを示しています。

```
ciscoasa# show service-policy | include dns
Inspect: dns preset_dns_map, packet 0, lock fail 0, drop 0, reset-drop 0
```

DNS インスペクションはデフォルトで有効になっています。

実行中のソフトウェア バージョンの確認

脆弱性のあるバージョンの Cisco ASA ソフトウェアがアプライアンスで実行されているかどうかを確認するには、**show version** コマンドを実行します。次の例は Cisco ASA ソフトウェア バージョン 8.4(1) を実行しているデバイスを示しています。

```
ciscoasa#show version | include Version
Cisco Adaptive Security Appliance Software Version 8.4(1)
Device Manager Version 6.4(1)
```

Cisco Adaptive Security Device Manager（ASDM）を使用してデバイスを管理している場合は、ログイン ウィンドウの表内、または Cisco ASDM ウィンドウの左上にソフトウェアのバージョンが表示されます。

脆弱性が認められない製品

Cisco ASA-CX Context-Aware Security は、これらの脆弱性の影響を受けません。

Cisco FWSM を除いて、これらの脆弱性の影響を受けるシスコ製品は現在確認されていません。

詳細

Cisco 適応型セキュリティ アプライアンス（ASA）ソフトウェアは、Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス、Cisco Catalyst 6500 シリーズ スイッチおよび Cisco 7600 シリーズ ルータ用の Cisco ASA Services Module（ASASM）と、Cisco ASA 1000V Cloud Firewall で使用されるオペレーティング システムです。Cisco ASA ファミリは、ファイアウォールや侵入防御システム（IPS）、anti-X、VPN などのネットワーク セキュリティ サービスを提供します。

Cisco ASA ソフトウェアには複数の脆弱性があり、認証されていないリモートの攻撃者が該当デバイスのリロードを引き起こす可能性があります。

IKE バージョン 1 における DoS 脆弱性

IKE バージョン 1 には実装面での脆弱性があり、認証されていないリモートの攻撃者が該当デバイスのリロードを引き起こす可能性があります。

この脆弱性は、受信した IKE バージョン 1 メッセージの不適切な処理に起因します。攻撃者は巧妙に細工した IKE メッセージを送信することで、この脆弱性を不正利用する可能性があります。この脆弱性を不正利用することにより、攻撃者は該当デバイスのリロードを引き起こすことができる場合があります。

この脆弱性の不正利用に使用できるのは、該当システム宛てのトラフィックのみです。シングルおよびマルチコンテキスト モードの両方における、ルーテッド ファイアウォール モードがこの脆弱性の影響を受けます。この脆弱性は、IPv4 および IPv6 トラフィックによって引き起こされる可能性があります。

この脆弱性は、Cisco Bug ID CSCub85692（ 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-2013-1149 が割り当てられています。

細工された URL における DoS 脆弱性

Cisco ASA ソフトウェア認証プロキシ機能の URL 処理コードには脆弱性が存在するため、認証されていないリモートの攻撃者によって該当デバイスのリロードが引き起こされる可能性があります。

この脆弱性は、細工された URL の誤った処理に起因します。攻撃者は細工した URL を該当デバイスに送信することで、この脆弱性を不正利用する可能性があります。この脆弱性を不正利用することにより、攻撃者はサービス拒否（DoS）状態を引き起こすことができる場合があります。

通過トラフィックと該当システム宛てのトラフィックの両方によって、この脆弱性が不正利用される可能性があります。シングルおよびマルチコンテキスト モードの両方における、ルーテッドおよび透過的ファイアウォール モードの両方に影響します。また、IPv4 および IPv6 トラフィックによって引き起こされる可能性があります。

この脆弱性は、Cisco Bug ID CSCud16590（ 登録ユーザ専用 ）として文書化され、CVE ID として CVE-2013-1150 が割り当てられています。

細工された証明書検証における DoS 脆弱性

認証のためのデジタル証明書検証に使用される機能には実装面での脆弱性が存在するため、認証されていないリモートの攻撃者によって該当デバイスのリロードが引き起こされる可能性があります。

この脆弱性は、認証中に使用されるデジタル証明書検証用のコードにある実装エラーに起因します。攻撃者は細工した証明書を使用して該当デバイスで認証操作を開始させることで、この脆弱性を不正利用する可能性があります。

この脆弱性の不正利用に使用できるのは、該当システム宛てのトラフィックのみです。シングルおよびマルチコンテキスト モードの両方における、ルーテッドおよび透過的ファイアウォール モードの両方に影響します。また、IPv4 および IPv6 トラフィックによって引き起こされる可能性があります。

この脆弱性は、Cisco Bug ID CSCuc72408（ 登録ユーザ専用 ）として文書化され、CVE ID として CVE-2013-1151 が割り当てられています。

DNS インスペクションにおける DoS 脆弱性

Cisco ASA ソフトウェア DNS アプリケーション インスペクションは、DNS スプーフィングとキャッシュ ポイズニングを防ぐための DNS メッセージ制御をサポートしています。

Cisco ASA ソフトウェアの DNS インスペクション エンジン コードには脆弱性が存在するため、認証されていないリモートの攻撃者によって該当デバイスのリロードが引き起こされる可能性があります。

この脆弱性は、DNS メッセージの一部フィールドの不適切な処理に起因します。攻撃者は該当デバイスによるインスペクションを開始させる細工したDNS メッセージを送信することで、この脆弱性を不正利用する可能性があります。

この脆弱性は、通過トラフィックによってのみ不正利用が可能で、 シングルおよびマルチコンテキスト モードの両方における、ルーテッドおよび透過的ファイアウォール モードの両方に影響します。また、IPv4 および IPv6 トラフィックによって引き起こされる可能性があります。

この脆弱性は、Cisco Bug ID CSCuc80080（ 登録ユーザ専用 ）として文書化され、CVE ID として CVE-2013-1152 が割り当てられています。

脆弱性スコア詳細

シスコはこのアドバイザリでの脆弱性に対して Common Vulnerability Scoring System（ CVSS ）に基づいたスコアを提供しています。本セキュリティ アドバイザリでの CVSS スコアは、CVSS バージョン 2.0 に基づいています。

CVSS は、脆弱性の重要度を示唆するもので、緊急性および対応の優先度を決定する組織の手助けとなる標準ベースの評価法です。

シスコでは、基本評価スコア（ Base Score ）および現状評価スコア（ Temporal Score ）を提供しています。お客様はこれらを用いて環境評価スコア（ Environmental Score ）を算出し、自身のネットワークにおける脆弱性の影響度を知ることができます。

シスコは次のリンクで CVSS に関する追加情報を提供しています。

http://www.cisco.com/web/about/security/intelligence/cvss-qandas.html

またシスコでは、各ネットワークにおける環境影響度を算出する CVSS 計算ツールを次のリンクで提供しています。

http://tools.cisco.com/security/center/cvssCalculator.x/

CSCub85692 -- IKE Version 1 Denial of Service Vulnerability Calculate the environmental score of					
CVSS Base Score - **7.8**					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	None	None	Complete
CVSS Temporal Score - **6.4**					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

CSCud16590-- ASA may Crash in thread emweb/https Calculate the environmental score of					
CVSS Base Score - **7.8**					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	None	None	Complete
CVSS Temporal Score - **6.4**					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

CSCuc72408-- Crash during certificate validation Calculate the environmental score of					
CVSS Base Score - **7.1**					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Medium	None	None	None	Complete
CVSS Temporal Score - **5.9**					
Exploitability		Remediation Level		Report Confidence	

Functional	Official-Fix	Confirmed

CSCuc80080-- ASA Unexpectedly Reloads in 'DATAPATH' Thread Calculate the environmental score of					
CVSS Base Score - **7.8**					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	None	None	Complete
CVSS Temporal Score - **6.4**					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

影響

このセキュリティ アドバイザリに記載されたいずれかの脆弱性について、不正利用が成功した場合、影響を受けるデバイスではリロードが発生することがあります。不正利用が繰り返されると、DoS 状態が続く可能性があります。

ソフトウェア バージョンおよび修正

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 Cisco Security Advisories, Responses, and Notices アーカイブや、後続のアドバイザリを参照して、起こりうる障害を判断し、それに対応できるアップグレード 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、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。

次の表に、すべての推奨リリースを記載します。これらの推奨リリースには、このアドバイザリに記載のあるすべての脆弱性の修正が含まれ･ﾄいます。シスコは「Recommended Releases」列のリリース、またはそれ以降のリリースにアップグレードすることを推奨します。

Major Release	Recommended Release
7.0	Migrate to 7.2.x or later
7.1	Migrate to 7.2.x or later
7.2	7.2(5.10)
8.0	8.0(5.31)
8.1	Migrate to 8.2.x or later
8.2	8.2(5.41)

8.3	8.3(2.37)
8.4	8.4(5.6)
8.5	Vulnerable; migrate to 9.x
8.6	8.6(1.10)
8.7	8.7(1.4)
9.0	9.0(2)
9.1	9.1(2)

次の表に、このアドバイザリで説明のある個別の脆弱性への修正を含む最初のリリースを記載します。各脆弱性に対する最初の修正リリースは異なるため、この一覧は情報の網羅を目的として提供されています。このアドバイザリで説明のあるすべての脆弱性への修正が含まれたリリースについては前の表を参照してください。

Vulnerability	Major Release	First-fixed Relea
IKE Version 1 Denial of Service Vulnerability (CSCub85692)	7.0	Migrate to 7.2.x or
	7.1	Migrate to 7.2.x or
	7.2	7.2(5.10)
	8.0	8.0(5.28)
	8.1	Migrate to 8.2.x or
	8.2	8.2(5.35)
	8.3	8.3(2.34)
	8.4	8.4(4.11)
	8.5	Not affected
	8.6	8.6(1.10)
	8.7	8.7(1.3)
	9.0	Not affected
	9.1	Not affected
Crafted URL Denial of Service Vulnerability (CSCud16590)	7.0	Migrate to 7.2.x or
	7.1	Migrate to 7.2.x or
	7.2	7.2(5.10)
	8.0	8.0(5.31)
	8.1	Migrate to 8.2.x or
	8.2	8.2(5.38)
	8.3	8.3(2.37)
	8.4	8.4(5.3)
	8.5	Vulnerable; migrate 9.x
	8.6	8.6(1.10)
	8.7	8.7(1.4)
	9.0	9.0(1.1)
	9.1	9.1(1.2)
Denial of Service During Validation of Crafted Certificates (CSCuc72408)	7.0	Migrate to 7.2.x or
	7.1	Migrate to 7.2.x or
	7.2	7.2(5.10)
	8.0	8.0(5.31)
	8.1	Migrate to 8.2.x or

	8.2	8.2(5.38)
	8.3	8.3(2.37)
	8.4	8.4(5)
	8.5	8.5(1.17)
	8.6	8.6(1.10)
	8.7	8.7(1.3)
	9.0	Not affected
	9.1	Not affected
DNS Inspection Denial of Service Vulnerability (CSCuc80080)	7.0	Not affected
	7.1	Not affected
	7.2	Not affected
	8.0	Not affected
	8.1	Not affected
	8.2	Not affected
	8.3	Not affected
	8.4	Not affected
	8.5	Not affected
	8.6	Not affected
	8.7	Not affected
	9.0	9.0(1.2)
	9.1	Not affected

ソフトウェアのダウンロード

Cisco ASA ソフトウェアは Cisco.com 内の Software Center からダウンロードできます。
http://www.cisco.com/cisco/software/navigator.html

Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンスについては、次の順に移動してください。[Products] > [Security] > [Firewalls] > [Adaptive Security Appliances (ASA)] > [Cisco ASA 5500 Series Adaptive Security Appliances] > [<ご利用の Cisco ASA モデル>] > [Adaptive Security Appliance (ASA) Software] これらバージョンの一部は暫定バージョンのため、ダウンロード ページの [Interim] タブに表示される場合があります。

Cisco Catalyst 6500 シリーズ スイッチおよび Cisco 7600 シリーズ ルータ用の Cisco ASA Services Module については、次の順に移動してください。[Products] > [Cisco Interfaces and Modules] > [Cisco Services Modules] >[Cisco Catalyst 6500 Series / 7600 Series ASA Services Module] > [Adaptive Security Appliance (ASA) Software] これらバージョンの一部は暫定バージョンのため、ダウンロード ページの [Interim] タブに表示される場合があります。

Cisco ASA 1000V Cloud Firewall については、次の順に移動してください。[Products] > [Security] > [Firewalls] > [Adaptive Security Appliances (ASA)] > [Cisco ASA 1000V Cloud Firewall] > [Adaptive Security Appliance (ASA) Software]

回避策

IKE バージョン 1 における DoS 脆弱性

可能であれば、IKE バージョン 1 を無効にすることで、この脆弱性を軽減できます。IKE バージョン 1 を無効にすると、IKE バージョン 1 を Security Association（SA）のネゴシエーションと

確立に使用するように設定されている IPsec ベースの VPN トンネル（LAN-to-LAN およびリモート アクセス）も無効になることに注意してください。ただし、管理者が SSL VPN のみ（リモート アクセスのみ）を使用する場合、VPN ソリューションに影響を与えずに IKE バージョン 1 を無効にすることができます。**no crypto isakmp enable <インターフェイス名>**（Cisco ASA ソフトウェア 8.3.x 以前）または **no crypto ikev1 enable <インターフェイス名>**（Cisco ASA ソフトウェア 8.4.x 以降）グローバル コンフィギュレーション コマンドで IKE バージョン 1 を無効にすることができます。

IKE バージョン 2 はこの脆弱性の影響を受けないため、IKE バージョン 2 に移行して IKE バージョン 1 を無効にすると、この脆弱性を排除できます。

細工された URL における DoS 脆弱性

可能であれば、ネットワーク アクセス制御用の AAA とネットワーク ユーザ認証用の HTTP(S) リスニング ポートを無効にすることで、この脆弱性を軽減できます。ネットワーク ユーザ認証用の HTTP(S) リスニング ポートは、**no aaa authentication listener** グローバル コンフィギュレーション コマンドで無効にすることができます。

細工された証明書検証における DoS 脆弱性

この脆弱性を軽減する対応策はありません。

DNS インスペクションにおける DoS 脆弱性

可能であれば、DNS インスペクションを無効にすることで、この脆弱性を軽減できます。次のコマンドを使用して、デフォルトで設定されている DNS インスペクションを無効にすることができます。

```
ciscoasa(config)# policy-map global_policy
ciscoasa(config-pmap)# class inspection_default
ciscoasa(config-pmap-c)# no inspect dns
```

修正済みソフトウェアの入手

シスコはこのアドバイザリに記載された脆弱性に対処する無償のソフトウェア アップデートを提供しています。ソフトウェアの導入を行う前に、お客様のメンテナンス プロバイダーにご相談いただくか、ソフトウェアのフィーチャ セットの互換性およびお客様のネットワーク環境の特有の問題をご確認ください。

お客様がインストールしたりサポートを受けたりできるのは、ご購入いただいたフィーチャ セットに対してのみとなります。そのようなソフトウェア アップグレードをインストール、ダウンロード、アクセスまたはその他の方法で使用した場合、お客様は http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html に記載のシスコのソフトウェア ライセンスの条項に従うことに同意したことになります。

サービス契約をご利用のお客様

サービス契約をご利用のお客様は、通常のアップデート チャネルからアップグレード ソフトウェアを入手してください。ほとんどのお客様は、 Cisco.com の Software Navigator からアップグレード ソフトウェアを入手できます。 http://www.cisco.com/cisco/software/navigator.html

サードパーティのサポート会社をご利用のお客様

シスコ パートナー、正規販売代理店、サービス プロバイダーなど、サードパーティのサポート会社と以前に契約していたか、または現在契約しており、その会社からシスコ製品の提供または保守を受けているお客様は、該当するサポート会社に連絡し、正しい処置についてのサポートを受けてください。

回避策や修正の効果は、使用している製品、ネットワーク トポロジー、トラフィックの性質や組織の目的などに関するお客様の状況によって異なります。影響を受ける製品やリリースは多種多様であるため、回避策を実施する前に、対象ネットワークで適用する回避策または修正が最適であることを、お客様のサービス プロバイダーやサポート会社にご確認ください。

サービス契約をご利用でないお客様

シスコから製品を直接購入したもののシスコのサービス契約をご利用いただいていない場合、または、サードパーティ ベンダーから購入したものの修正済みソフトウェアを購入先から入手できない場合は、Cisco Technical Assistance Center（TAC）に連絡してアップグレード ソフトウェアを入手してください。

- +1 800 553 2447（北米からの無料通話）
- +1 408 526 7209（北米以外からの有料通話）
- E メール：tac@cisco.com

無償アップグレードの対象製品であることを証明していただくために、製品のシリアル番号と、本アドバイザリの URL をご用意ください。サービス契約をご利用でないお客様は TAC に無償アップグレードをリクエストしてください。

多言語による各地の電話番号、説明、E メール アドレスなどの TAC の連絡先情報については、Cisco Worldwide Contact を参照してください。
http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html

不正利用事例と公式発表

Cisco Product Security Incident Response Team（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とその公表は確認しておりません。

このセキュリティ アドバイザリに記載された脆弱性はすべて、カスタマー サポート ケースの解決中に発見されたものです。

この通知のステータス：FINAL

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を示唆するものでもありません。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。またシスコはいつでも本ドキュメントの変更や更新を実施する権利を有します。

後述する情報配信の URL を省略し、本アドバイザリの記述内容に関して単独の転載や意訳を実施した場合には、事実誤認ないし重要な情報の欠落を含む統制不可能な情報の伝搬が行われる可能性があります。

情報配信

このアドバイザリは次のリンクにある Cisco Security Intelligence Operations に掲載されます。

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130410-asa/

また、このアドバイザリのテキスト版が Cisco PSIRT PGP キーによるクリア署名つきで次の E メールで配信されています。

- cust-security-announce@cisco.com
- first-bulletins@lists.first.org
- bugtraq@securityfocus.com
- vulnwatch@vulnwatch.org
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- full-disclosure@lists.grok.org.uk

本アドバイザリに関する今後の更新は Cisco.com に掲載されますが、メーリング リストで配信されるとは限りません。更新内容については、本アドバイザリの URL でご確認ください。

更新履歴

Revision 1.1	2013-May-23	Made Cisco ASA Software release 9.1(2) the recommended 9.1.x release because the previous 9.1.x recommended release (9.1.1.4) was reported to be unstable in certain configurations. This instability issue is fixed in release 9.1(2).
Revision 1.0	2013-April-10	Initial public release.

シスコ セキュリティ手順

シスコ製品におけるセキュリティの脆弱性の報告、セキュリティ事故に関するサポート、およびシスコからセキュリティ情報を入手するための登録方法の詳細については、Cisco.com の http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html を参照してください。この Web ページには、シスコのセキュリティ アドバイザリに関してメディアが問い合わせる際の指示が掲載されています。シスコ セキュリティ アドバイザリについては、すべて http://www.cisco.com/go/psirt/ で確認できます。