Multiple Vulnerabilities in Cisco IPS Software

Advisory ID: cisco-sa-20140219-ips

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140219-ips

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 1.0

For Public Release 2014 February 19 16:00 UTC (GMT)

目次

要約

Cisco Intrusion Prevention System（IPS）ソフトウェアは、次の脆弱性の影響を受けます。

- Cisco IPS 分析エンジンの DoS 脆弱性
- Cisco IPS Control-Plane の MainApp の Dos 脆弱性
- Cisco IPS のジャンボ フレームの DoS 脆弱性

Cisco IPS 分析エンジンの DoS 脆弱性と、Cisco IPS ジャンボ フレームの DoS 脆弱性により、認証されていないリモートの攻撃者によって *Analysis Engine* プロセスが応答不能にさせられる可能性があります。この状況が発生すると、Cisco IPS はトラフィックの検査を停止します。

Cisco IPS Control-Plane の MainApp の Dos 脆弱性により、認証されていないリモート攻撃者によって *MainApp* プロセスが応答不能にさせられ、アラート通知、イベント ストアの管理、センサーの認証などのタスクが実行不能になる可能性があります。また、 *MainApp* プロセスが応答不能になっている場合は Cisco IPS の Web サーバも使用できなくなり、また *Analysis Engine* プロセスなどの他のプロセスも正しく機能しない場合があります。

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。この中のいくつかの脆弱性には影響を軽減する回避策が存在します。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-20140219-ips

該当製品

脆弱性が認められる製品

Cisco IPS 分析エンジンの DoS 脆弱性

次の製品は、Cisco IPS 分析エンジンの DoS 脆弱性の影響を受けます。

- Cisco ASA 5500-X シリーズ IPS セキュリティ サービス プロセッサ（IPS SSP）ソフトウェアおよびハードウェア モジュール
- Cisco ASA 5500 シリーズ Advanced Inspection and Prevention セキュリティ サービス モジュール（AIP SSM）
- Cisco IPS 4200 シリーズ センサー
- Cisco IPS 4300 シリーズ センサー
- Cisco IPS 4500 シリーズ センサー

この脆弱性は、7.1(4)E4 よりも前の Cisco IPS ソフトウェア リリースには影響しません。

この脆弱性の影響を受けるのは、**produce-verbose-alert** アクションが有効になっているシグニチャで設定された Cisco IPS ソフトウェアか、または、このアクションを追加するためにイベント アクション オーバーライド（EAO）が設定されているシステムだけです。

produce-verbose-alert オプションがアクティブ シグニチャまたは EAO 設定で使用されているかどうかを確認するには、**show configuration** コマンドを使用します。

次の例は、**produce-verbose-alert** オプションを有効にするために変更されたシグニチャ ID 1475/0 を示しています。

```
sensor# show configuration
! ------------------------------
! Current configuration last modified Wed Feb 05 16:21:00 2014
! ------------------------------
! Version 7.1(8)
! Host:
! Realm Keys key1.0
[...]

variables WEBPORTS web-ports 24326-24326,3128-3128,80-80,8000-8000,8010-
8010,8080-8080,8888-8888
signatures 1475 0
engine string-tcp
event-action produce-alert|produce-verbose-alert
```

```
exit

[...]
```

次の例は、**produce-verbose-alert** オプションでオーバーライドが有効になっているイベント アクション ルール ポリシー *rules0* を示しています。

```
sensor# show configuration
! ------------------------------
! Current configuration last modified Wed Feb 05 16:21:00 2014
! ------------------------------
! Version 7.1(8) ! Host: ! Realm Keys key1.0 [...] ! ----------------------
-------- service event-action-rules rules0 overrides deny-packet-inline
override-item-status Enabled risk-rating-range 90-100 exit overrides
produce-verbose-alert override-item-status Enabled risk-rating-range 90-100
exit exit ! ------------------------------
[...]
```

また、いずれかのアクティブ シグニチャで **produce-verbose-alert** オプションが有効になっているかどうかを確認するには、Cisco IPS Device Manager（IDM）を使用して Cisco IPS に接続し、**[Configuration]、[Policies]、[Signature Definitions]、[-Sig-Definition-Name-]、[Active Signatures]** の順に移動して、Filter: Action **Produce Verbose Alert** を使用してフィルタリングします。

produce-verbose-alert オプションは、アクション シグニチャでも EAO ルールでも、デフォルトでは有効になっていません。

Cisco IPS Control-Plane の MainApp の Dos 脆弱性

次の製品は、Cisco IPS Control-Plane の MainApp の Dos 脆弱性の影響を受けます。

- Cisco ASA 5505 Advanced Inspection and Prevention セキュリティ サービス カード（AIP SSC）
- Cisco ASA 5500 シリーズ Advanced Inspection and Prevention セキュリティ サービス モジュール（AIP SSM）
- Cisco ASA 5500-X シリーズ IPS セキュリティ サービス プロセッサ（IPS SSP）ソフトウェアおよびハードウェア モジュール

注： Cisco ASA 5505 用 Advanced Inspection and Prevention セキュリティ サービス カード（AIP SSC）は、ソフトウェア メンテナンス終了となっています。代替製品に関しては、シスコの担当者までお問い合わせください。

Cisco IPS のジャンボ フレームの DoS 脆弱性

次の製品は、Cisco IPS のジャンボ フレームの DoS 脆弱性の影響を受けます。

- Cisco IPS 4500 シリーズ センサー

実行中のソフトウェア バージョンを知る方法

脆弱性のあるバージョンの Cisco IPS 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、ソフトウェア バージョン

7.1(3)E4 を実行している Cisco IPS 4345 を示しています。

```
sensor# show version
Application Partition:

Cisco Intrusion Prevention System, Version 7.1(3)E4

Host:
Realm Keys key1.0
Signature Definition:
Signature Update S605.0 2011-10-25
OS Version: 2.6.29.1
Platform: IPS-4345-K9
```

Cisco Intrusion Prevention System Device Manager（IDM）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 IDM 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

他のシスコ製品においてこの脆弱性の影響を受けるものは、現在確認されていません。

詳細

Cisco IPS は、ネットワークベースの脅威防止サービスを提供するネットワーク セキュリティ デバイス ファミリです。Cisco IPS ソフトウェアには、システムがさまざまなタスクを実行するために使用するアプリケーションが含まれています。特に *MainApp* プロセスは、設定の読み込みや、アプリケーションおよび認証サービスの開始と停止など、複数の重要なタスクを処理します。一方、Analysis Engine プロセスは、ルータを通過するトラフィックの分析と検査を実行します。

MainApp プロセスと Analysis Engine プロセスの追加情報については、製品の設定ガイドの「システム アーキテクチャ」セクションを参照してください。
http://www.cisco.com/en/US/docs/security/ips/7.1/configuration/guide/idm/idm_system_architecture.html#wp1126061

Cisco IPS 分析エンジンの DoS 脆弱性

Cisco Intrusion Prevention System（IPS）ソフトウェアの **produce-verbose-alert** コードの脆弱性により、認証されていないリモート攻撃者によって Analysis Engine プロセスが応答不能にさせられる可能性があります。

この脆弱性は、 **produce-verbose-alert** アクションが有効になっているときに Analysis Engine プロセスが行うフラグメント化されたパケットの処理が不適切であることに起因します。攻撃者は、フラグメント化されたパケットを該当システムを介して送信することで、この脆弱性を不正利用する可能性があります。この脆弱性を引き起こすために、攻撃者は **produce-verbose-alert** アクションでシグニチャを起動するか、 **produce-verbose-alert** がイベント アクション オーバーライドとして設定されているイベントをトリガーする可能性があります。この不正利用により、攻撃者によって Analysis Engine プロセスが応答不能にさせられる可能性があります。これにより、該当システムがトラフィックの検査を停止します。

この脆弱性は、該当システムを通過するフラグメント化された IP バージョン 4（IPv4）および IP バージョン 6（IPv6）パケットによって引き起こされる可能性があります。Cisco IPS の管理 IP アドレスを宛先とするトラフィックは、この脆弱性を引き起こしません。

この脆弱性は、Cisco Bug ID CSCui91266（ 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-2014-0718 が割り当てられています。

Cisco IPS Control-Plane の MainApp の Dos 脆弱性

Cisco IPS ソフトウェアのコントロールプレーン アクセス リストの実装の脆弱性により、認証されていないリモート攻撃者によって *MainApp* プロセスが応答不能にさせられる可能性があります。

この脆弱性は、該当システムの管理 IP アドレスに送信された不正な TCP パケットを適切に処理できないことに起因します。攻撃者は、巧妙に細工した TCP パケットを管理インターフェイスの IP アドレスの TCP ポート 7000 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。この不正利用により、攻撃者は *MainApp* プロセスを応答不能にできる可能性があります。このため、Cisco IPS センサーでは警告の通知、イベント ストアの管理、センサーの認証など、いくつかの重要なタスクが実行できなくなり、Denial of Service（DoS）状態が発生することがあります。また、 *MainApp* プロセスが応答不能になっているときは、Cisco IPS の Web サーバも使用できなくなります。さらに、この全般的なシステム障害によって、Analysis Engine などの他のプロセスが正しく機能しなくなることがあります。

この脆弱性は、管理インターフェイスの IP アドレスの TCP ポート 7000 を宛先とする TCP トラフィックによってのみ引き起こされます。センシング インターフェイスを通過するトラフィックは、この脆弱性を引き起こしません。Cisco IPS が無差別モードに設定されている場合は、 **shun** や **rate-limit** などの *MainApp* の処理を必要とする緩和アクションは 利用できなくなることがあります。Cisco IPS がインライン モードに設定されている場合は、Analysis Engine プロセスが正しく機能しないことがあるため、センサーでインスペクションおよび緩和アクションが正しく実行されない可能性があります。

この脆弱性の影響を受けるのは、Cisco ASA 5500 シリーズおよび Cisco ASA 5500-X シリーズ用ハードウェア モジュールとソフトウェア モジュール上で動作する Cisco IPS ソフトウェアだけです。

この脆弱性は、Cisco Bug ID CSCui67394（ 登録ユーザ専用）として文書化され、CVE ID として CVE-2014-0719 が割り当てられています。

Cisco IPS のジャンボ フレームの DoS 脆弱性

ジャンボ フレームを処理する Cisco IPS コードの脆弱性により、認証されていないリモート攻撃者によって Analysis Engine プロセスが応答不能にさせられる可能性があります。

この脆弱性は、高速で送信されるジャンボ フレームの処理が不適切なことに起因します。攻撃者は、該当デバイスのセンシング インターフェイスを介してジャンボ フレームを送信することで、この脆弱性を不正利用する可能性があります。この不正利用により、攻撃者によって Analysis Engine プロセスが応答不能にさせられる可能性があります。これにより、該当システムがトラフィックの検査を停止します。

この脆弱性は、該当システムを通過する IPv4 および IPv6 ベースのジャンボ フレームによって引き起こされます。Cisco IPS の管理 IP アドレスを宛先とするトラフィックは、この脆弱性を引き起こしません。

この脆弱性は、Cisco Bug ID CSCuh94944（ 登録ユーザ専用）として文書化され、CVE ID として CVE-2014-0720 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/

CSCui91266 - Cisco IPS Analysis Engine Denial of Service Vulnerability 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	

CSCui67394 - Cisco IPS Control-Plane MainApp 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 - **6.8**		
Exploitability	Remediation Level	Report Confidence
High	Official-Fix	Confirmed

CSCuh94944 - Cisco IPS Jumbo Frame Denial of Service Vulnerability 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	

影響

Cisco IPS 分析エンジンの DoS 脆弱性および Cisco IPS のジャンボ フレームの DoS 脆弱性の不正利用に成功した場合、*Analysis Engine* プロセスを応答不能にできる可能性があります。この状況が発生すると、Cisco IPS はトラフィックの検査を停止します。

Cisco IPS Control-Plane の MainApp の Dos 脆弱性が不正利用されると、*MainApp* プロセスが応答不能になり、アラート通知、イベント ストアの管理、センサーの認証などのタスクを実行できなくなる可能性があります。また、*MainApp* プロセスが応答不能になっている場合は Cisco IPS の Web サーバも使用できなくなり、また Analysis Engine プロセスなどの他のプロセスも正しく機能しない場合があります。

Cisco IPS が無差別モードに設定されている場合は、**shun** や **rate-limit** などの *MainApp* の処理を必要とする緩和アクションは利用できなくなることがあります。Cisco IPS がインライン モードに設定されている場合は、Analysis Engine プロセスが正しく機能しないことがあるため、センサーでインスペクションおよび緩和アクションが正しく実行されない可能性があります。該当システムの全機能を復元するためにはリロードが必要です。

さらに、影響を受けるバージョンのソフトウェアを実行している Cisco IPS モジュールを使用した Cisco ASA がハイ アベイラビリティ（HA）モードに設定されている場合は、*MainApp* が応答不能になるとフェールオーバー イベントが引き起こされる可能性があります。

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。

次の表は、各脆弱性の最初の修正リリースとメジャー リリース バージョンをまとめたものです。最後の行には、このセキュリティ アドバイザリに記載されているすべての脆弱性を解決する推奨リリースに関する情報を示しています。

	6.x	7.0	7.1	7.2	7.3
Cisco IPS Analysis Engine Denial of Service Vulnerability - CSCui91266	Not Affected	Not Affected	7.1(8)E4[1]	7.2(2)E4	Not Affected
Cisco IPS Control-Plane MainApp Denial of Service Vulnerability - CSCui67394	Affected, move to 7.1 or later[2]	Affected, move to 7.1 or later	7.1(8p2)E4	7.2(2)E4	Not Affected
Cisco IPS Jumbo Frame Denial of Service Vulnerability - CSCuh94944	Not Affected	Not Affected	7.1(8)E4	7.2(2)E4	Not Affected
Recommended Release	**Affected, move to 7.1 or later**	**Affected, move to 7.1 or later**	**7.1(8p2)E4 or later**	**7.2(2)E4 or later**	**Not Affected**

[1] この脆弱性は、7.1(4)E4 よりも前の Cisco IPS ソフトウェア バージョンには影響しません。
[2] Cisco ASA 5505 Advanced Inspection and Prevention セキュリティ サービス カード（AIP SSC）がサポートしているのは、Cisco IPS ソフトウェア バージョン 6.2 以前のみです。Cisco ASA 5505 用 Advanced Inspection and Prevention セキュリティ サービス カード（AIP SSC）は、ソフトウェア メンテナンス終了となっています。

回避策

Cisco IPS 分析エンジンの DoS 脆弱性を回避するために、管理者は **produce-verbose-alert** アクションを無効にすることができます。

show configuration コマンドを使用して、 **produce-verbose-alert** オプションが有効になっているシグニチャを確認したり、 **produce-verbose-alert** オプションが EAO として有効になっているかを確認します。

produce-verbose-alert がシグニチャ レベルで設定されている場合は、シグニチャ設定プロンプトを入力して、変更が必要な各シグニチャのイベント アクションを変更することで、 **produce-verbose-alert** の代わりに **produce-alert** を使用するよう変更できます。次の例は、シグニチャ 1475/0 のイベント アクションを **produce-verbose-alert** から **produce-alert** に変更する手順を示しています。

```
sensor(config)# service signature-definition sig0
sensor(config-sig)# signatures 1475 0
sensor(config-sig-sig)# engine string-tcp
sensor(config-sig-sig-str)# event-action produce-alert
sensor(config-sig-sig-str)# exit
sensor(config-sig-sig)# exit
sensor(config-sig)# exit
Apply Changes?[yes]: yes
```

```
sensor(config)#
```

また、管理者は **produce-verbose-alert** オプションが有効になっているアクティブなシグニチャを確認するために、Cisco Intrusion Prevention System Device Manager（IDM）を使用して Cisco IPS に接続し、 **[Configuration]、[Policies]、[Signature Definitions]、[-Sig-Definition-Name-]、[Active Signatures]** の順に移動し、Filter: Action **Produce Verbose Alert** を使用してフィルタリングできます。

シグニチャごとに、右クリックして **[Edit Action]** を選択します。パネルから **[Produce Verbose Alert]** チェック ボックスをオフにし、 **[OK]** をクリックして変更を適用します。

produce-verbose-alert アクションが EAO として有効になっている場合は、イベント アクション ルール ポリシーの設定を変更して、無効にすることができます。

次の例は、イベント アクション ルール ポリシー *rules0* で設定されている **produce-verbose-alert** でオーバーライドを無効にする方法を示しています。

```
sensor(config)# service event-action-rules rules0
sensor(config-eve)# no overrides produce-verbose-alert
sensor(config-eve)# exit
Apply Changes?[yes]: yes
sensor(config)#
```

Cisco IPS Control-Plane の MainApp の Dos 脆弱性を回避する方法はありませんが、許容されるホストの数を制限することで、この脆弱性による問題の発生を減少させることができます。

許容されるホストの数を制限するためには、管理者は **access-list** コマンドを使用する必要があります。リストからホストやネットワークを削除するには、 **no access-list** コマンドを使用する必要があります。
次の例は、完全な 192.168.1.0/24 ネットワークへのアクセス権を削除して、IP アドレスが 192.168.1.1 のホストへのアクセスのみを許可するコマンドのシーケンスを示しています。

- network-setting 設定モードで **show settings** コマンドを使用して、現在許可されているホストやネットワークを確認します。次の例は、192.168.1.0/24 ネットワーク内のすべてのホストを許可するように Cisco IDSM-2 が設定されていることを示しています。

```
sensor(config-hos-net)# show settings
network-settings
-----------------------------------------------
[...]
access-list (min: 0, max: 512, current: 1)
-----------------------------------------------
network-address: 192.168.1.0/24
-----------------------------------------------
-----------------------------------------------
ftp-timeout: 300 seconds <defaulted>
login-banner-text: <defaulted>
[...]
```

- network-setting 設定モードで **access-list** コマンドを使用して、192.168.1.1 ホストを追加します。

注：これが許可されている唯一のホストである場合は、必ずそのホストからコンフィギュレーション コマンドを実行するようにして、Cisco IDSM-2 モジュールへの接続が失われることを回避してください。

```
sensor(config-hos-net)#access-list 192.168.1.1/32
```

- network-setting 設定モードで **no access-list** コマンドを使用して、許可されているホスト リストの 192.168.1.0/32 ネットワークを削除します。

```
sensor(config-hos-net)#no access-list 192.168.1.0/24
```

- network-setting 設定モードで **show settings** コマンドを使用して、許可されているホストのリストが正しいことを確認します。

```
sensor(config-hos-net)# show settings
network-settings
-----------------------------------------------
[...]
access-list (min: 0, max: 512, current: 1)
-----------------------------------------------
network-address: 192.168.1.1/32
-----------------------------------------------
-----------------------------------------------
ftp-timeout: 300 seconds <defaulted>
login-banner-text: <defaulted>
[...]
```

- 設定を終了し、適用します。

```
sensor(config-hos-net)# exit
sensor(config-hos)# exit
Apply Changes:?[yes]:
```

Cisco IPS のジャンボ フレームの DoS 脆弱性の回避策はありません。

ネットワーク内のシスコ デバイスに適用可能な他の対応策は、このアドバイザリの付属ドキュメントである『Cisco Applied Intelligence』にて参照できます。
http://tools.cisco.com/security/center/viewAMBAlert.x?alertId=32605

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を入手することができます。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。

さまざまな言語向けの各地の電話番号、説明、電子メール アドレスなどの、この他の TAC の連絡先情報については、シスコ ワールドワイドお問い合わせ先（http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html）を参照してください。

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。

Cisco IPS 分析エンジンの DoS 脆弱性と、Cisco IPS Control-Plane の MainApp の Dos 脆弱性は、お客様からのお問い合わせへの対応の際に発見されました。Cisco IPS のジャンボ フレームの DoS 脆弱性は、シスコの社内テストで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-20140219-ips

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 1.0	2014-February-19	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/web/about/security/psirt/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。すべてのシスコ セキュリティ アドバイザリは、http://www.cisco.com/go/psirt/ で確認することができます。