Cisco 侵入防御システム システム・ソフトウェアの多重 脆弱点

High

アドバイザリーID : cisco-sa-20130717-ips

初公開日 : 2013-07-17 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 : CSCuh27460 CSCue51272 CSCtx18596 CSCua61977

CVE-2013-3410 CVE-2013-3411 CVE-2013-1243 CVE-2013-1218

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 侵入防御システム（IPS）ソフトウェアは次の脆弱性から影響を受けます:

- Cisco IPS ソフトウェア 不正 な IP パケット サービス拒否の脆弱性
- Cisco IPS ソフトウェア 断片化したトラフィック サービス拒否の脆弱性
- Cisco IPS NME 不正 な IP パケット サービス拒否の脆弱性
- Cisco IDSM-2 不正 な TCP パケット サービス拒否の脆弱性

Cisco IPS ソフトウェア 不正 な IP パケット サービス拒否の脆弱性はリモート攻撃者非認証により *MainApp* プロセスは無理解になりますする可能性があります。

Cisco IPS ソフトウェア 断片化したトラフィック サービス拒否の脆弱性は非認証、リモート攻撃者により *分析 エンジン* プロセスはメモリ不良が無理解な原因になりますことを可能にする可能性がありますまたは影響を受けたシステムのリロードを引き起こす可能性があります。

高められた Cisco IPS NME 不正 な IP パケット サービス拒否の脆弱性はリモート攻撃者非認証により Cisco 侵入防御システム ネットワーク モジュールのリロードを引き起こすようにする可能性があります（IPS NME）。

Cisco IDSM-2 不正 な TCP パケット サービス拒否の脆弱性はリモート攻撃者非認証により Cisco Catalyst 6500 シリーズ Intrusion Detection System （IDSM-2）モジュールのカーネルは無理解に

なりますする可能性があります。

これらの脆弱性の何れかの不正利用の成功はサービス拒否（DoS）状態という結果に終る可能性があります。

Cisco は Cisco IDSM-2 不正 な TCP パケット サービス拒否の脆弱性を除いてこのアドバイザリのすべて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ました。 Cisco IDSM-2 モジュールの脆弱なバージョンを実行している顧客は利用可能 な軽減のためのこのアドバイザリの「回避策」セクションを参照する必要があります。

Cisco IPS ソフトウェア 断片化したトラフィック サービス拒否の脆弱性および Cisco IDSM-2 不正 な TCP パケット サービス拒否の脆弱性を軽減する回避策は利用できます。

このアドバイザリは、次のリンクより確認できます。
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130717-ips

該当製品

脆弱性のある製品

Cisco IPS ソフトウェア 不正 な IP パケット サービス拒否の脆弱性

以下の製品は Cisco IPS ソフトウェア 不正 な IP パケット サービス拒否の脆弱性から影響を受けます:

- バージョン 7.1(4)E4 を通して Cisco IPS ソフトウェア 7.1 を実行する 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エアモジュール
- Cisco IPS ソフトウェア バージョン 7.1(4)E4 を実行する Cisco IPS 4500 シリーズ センサー
- Cisco IPS ソフトウェア バージョン 7.1(3)E4 および 7.1(4)E4 を実行する Cisco IPS 4300 シリーズ センサー

注: この脆弱性は Cisco IPS ソフトウェア バージョン 7.1 を実行する製品だけ影響を及ぼします。 Cisco IPS ソフトウェア バージョン 7.0 およびそれ以前を実行する製品は影響を受けていません。

Cisco IPS ソフトウェア 断片化したトラフィック サービス拒否の脆弱性

以下の製品は Cisco IPS ソフトウェア 断片化したトラフィック サービス拒否の脆弱性から影響を受けます:

- Cisco IPS ソフトウェア バージョン 7.1(4)E4 によって 7.1(7)E4 を実行する Cisco ASA 5500-X シリーズ（IPS SSP）ソフトウエアモジュール

注: Cisco IPS ソフトウェア 断片化したトラフィック サービス拒否の脆弱性影響 Cisco ASA 5500-X シリーズ IPS SSP ソフトウエアモジュールだけ; Cisco ASA 5585-X のための Cisco IPS SSP ハードウエアモジュールはこの脆弱性から影響を受けません。

Cisco IPS NME 不正 な IP パケット サービス拒否の脆弱性

以下の製品は Cisco IPS NME 不正 な IP パケット サービス拒否の脆弱性から影響を受けます:

- 高められる Cisco 侵入防御システム ネットワーク モジュール（IPS NME）

Cisco IDSM-2 不正 な TCP パケット サービス拒否の脆弱性

以下の製品は Cisco IDSM-2 不正 な TCP パケット サービス拒否の脆弱性から影響を受けます:

- Cisco Catalyst 6500 シリーズ Intrusion Detection System（IDSM-2）モジュール

実行ソフトウェア バージョンの判別方法

Cisco IPS ソフトウェアの脆弱なバージョンがアプライアンスで動作しているかどうか判別するために、管理者は **show version コマンドを**発行できます。 ソフトウェア バージョン 7.1(3)E4 を実行している次の例は Cisco IPS 4345 を示したものです:

```
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 侵入防御システム デバイスマネージャ（IDM）をデバイスを管理するのに使用する顧客は Cisco IDM ウィンドウの Login ウィンドウか左上コーナーで表示する 表でソフトウェア バージョンを見つけることができます。

脆弱性を含んでいないことが確認された製品

以下の製品はこのアドバイザリに説明がある脆弱性から影響を受けません:

- Cisco IOS IPS
- Cisco IPS 4200 シリーズ センサー
- Cisco 侵入防御システム Advanced Integration Module（IPS AIM）
- Cisco ASA 5500 シリーズ高度インスペクションおよび防止セキュリティ サービス カード（AIP SSC）
- Cisco ASA 5500 シリーズ高度インスペクションおよび防止セキュリティ サービス モジュール（AIP SSM）

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 IPS ソフトウェア 不正 な IP パケット サービス拒否の脆弱性

Cisco IPS はネットワークベース 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 デバイスの系列です。 Cisco IPS ソフトウェアは異なるタスクを実行するのにシステムによって使用する複数の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、開始し、停止アプリケーションおよび認証サービス読むことを含む複数の重要なタスクに責任があります。

MainApp プロセスについてのその他の情報は製品構成 ガイドの「システムアーキテクチャ」セクションにあります: http://www.cisco.com/en/US/docs/security/ips/7.1/configuration/guide/idm/idm_system_architecture.html#wp1126061

IPスタックの脆弱性はリモート攻撃者非認証により *MainApp* プロセスは無理解になりますする可能性があります。 これは Cisco IPS センサーがアラート 通知、イベント ストア 管理およびセンサー認証を含む複数の重要なタスクを実行できないのでサービス拒否 （ DoS ）状態を作成します。 Cisco IPS Webサーバはまた *MainApp* プロセスが無理解な間、利用できないです。 さらに、この総合システム失敗が原因で、 *分析 エンジン*のような他のプロセスはきちんとはたらかないかもしれません。 脆弱性は影響を受けたシステムのマネージメントインターフェイスからの不正 な IP パケットの不適当な処理が原因です。 攻撃者はマネージメントインターフェイスへ不正 な IP パケットを送信 することによってこの脆弱性を不正利用することができます。

脆弱性はマネージメントインターフェイスに送信される IPv4 トラフィックによってだけ引き起こすことができます。 検知インターフェイスを通るトラフィックはこの脆弱性を引き起こしません。 Cisco IPS が混合モードで設定される場合場合、処理する *MainApp* を **排除する**必要とすれば **レート制限は**利用できないかもしれません軽減操作。 Cisco IPS がインライン モードで設定される場合、センサーは *分析 エンジン* プロセスがきちんとはたらかないかもしれないので正しくインスペクションおよび軽減操作を行わないかもしれません。

この脆弱性は Cisco バグ ID CSCtx18596 （ 登録ユーザのみ ）でおよびよくある脆弱性および公開（ CVE ） ID CVE-2013-1243 文書化されています。

Cisco IPS ソフトウェア 断片化したトラフィック サービス拒否の脆弱性

Cisco IPS SSP は ASA 5500-X シリーズを on Cisco 実行する統合されたモジュールです。 モジュールは Cisco ASA 5585-X のための、または Cisco ASA 5512-X、Cisco ASA 5515-X、Cisco ASA 5525-X、Cisco ASA 5545-X、および Cisco ASA 5555-X シリーズ用の統合 ソフト モジュールとしてハードウェアで配置できます。

ASA 5500-X IPS SSP で動作する Cisco IPS ソフトウェアは Cisco ASA から受信するトラフィックだけ処理します。 Cisco ASA は Cisco IPS ソフトウェアに特定のトラフィックをリダイレクト

するためにモジュラ 政策の枠組（MPF）で設定される必要があります。

断片化したトラフィックを処理するコードの実装の脆弱性は非認証、リモート攻撃者により *分析エンジン* プロセスは無理解になるか、または影響を受けたシステムをリロードさせますことを可能にする可能性があります。

脆弱性は Cisco ASA データ平面からインスペクションおよび処理のための Cisco IPS プロセッサに送信されるフラグメント化された IP パケットの不適当な処理が原因です。 攻撃者は影響を受けたシステムによってフラグメント化され、他の IP パケットの組み合せの送信によってこの脆弱性を不正利用する可能性があります。 エクスプロイトにより攻撃者が影響を受けたシステムのリロードを引き起こすか、または *分析 エンジン* プロセスを無理解にならせますことを可能にする可能性があります。 *分析 エンジン* プロセスが無理解なとき、影響を受けたシステムはこと廃棄されるべきトラフィック引き起こすトラフィックを処理しません。 影響を受けたソフトウェアのバージョンを実行するハイアベイラビリティ モード（HA）で Cisco IPS SSP ソフトウエアモジュールが付いている Cisco ASA が設定されればさらに、フェールオーバー イベントは Cisco IPS SSP がリロードするか、またはトラフィックを転送することを止めるとき引き起こされるかもしれません。

脆弱性は影響を受けたシステムを通る IPv4 および IPv6 フラグメント化されたパケットによって引き起こすことができます。 Cisco IPS ソフトウエアモジュールの管理IPアドレスへのトラフィック 誘導はこの脆弱性を引き起こしません。

注: この脆弱性は Cisco ASA 5500-X シリーズ IPS SSP ソフトウエアモジュールだけ影響を与えます。 Cisco ASA5585-X シリーズでサポートされる Cisco IPS SSP ハードウエアモジュールはこの脆弱性から影響を受けません。

この脆弱性は Cisco バグ ID CSCue51272（ 登録ユーザのみ）で文書化されています、CVE ID CVE-2013-1218 を割り当てられました。

Cisco IPS NME 不正 な IP パケット サービス拒否の脆弱性

メモリ 割り当てコードの脆弱性はリモート攻撃者非認証により影響を受けたシステムのリロードを引き起こすようにする可能性があります。 脆弱性は不正 な IP パケットが影響を受けたシステムのマネージメントインターフェイスで受信されるときメモリ 割り当ての不適当な処理が原因です。 攻撃者は管理IPアドレスへ不正 な IP パケットを送信 することによってこの脆弱性を不正利用することができます。

脆弱性はマネージメントインターフェイスに送信される IPv4 トラフィックによってだけ引き起こすことができます。 検知インターフェイスを通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 IPS NME を on Cisco 実行する Cisco IPS ソフトウェアだけ影響を与えます。

この脆弱性は Cisco バグ ID CSCua61977 （ 登録ユーザのみ ）で文書化されています、CVE ID CVE-2013-3410 を割り当てられました。

Cisco IDSM-2 不正 な TCP パケット サービス拒否の脆弱性

IDSM-2 ドライバの脆弱性はリモート攻撃者非認証によりシステム カーネルは無理解になりますする可能性があります。 これは Cisco IPS センサーがアラート 通知、イベント ストア 管理、センサー認証およびトラフィック インスペクションを含む複数の重要なタスクを、実行できないのでサービス拒否 （ DoS ）状態を作成します。 Cisco IPS Webサーバはまた利用できないです。

脆弱性は影響を受けたシステムのマネージメントインターフェイスからの不正 な TCP パケットの不適当な処理が原因です。 攻撃者はマネージメントインターフェイスへ不正 な IP パケットを送信 することによってこの脆弱性を不正利用することができます。 TCP 3 ウェイ ハンドシェイクがこの脆弱性を不正利用するために必要となりません。 ハード システム再度ブートするは必要システムの機能を回復するためにです。

脆弱性はマネージメントインターフェイスに送信される IPv4 トラフィックによってだけ引き起こすことができます。 検知インターフェイスを通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 IDSM-2 モジュールを on Cisco 実行する Cisco IPS ソフトウェアだけ影響を与えます。

この脆弱性は Cisco バグ ID CSCuh27460 （ 登録ユーザのみ ）で文書化されています、CVE ID CVE-2013-3411 を割り当てられました。

セキュリティ侵害の痕跡

回避策

Cisco IPS ソフトウェア 不正 な IP パケット サービス拒否の脆弱性および Cisco IPS NME 不正 な IP パケット サービス拒否の脆弱性

この脆弱性を軽減する回避策がありません。

Cisco IPS ソフトウェア 断片化したトラフィック サービス拒否の脆弱性

この脆弱性のエクスプロイトによりトラフィック割り込みを引き起こす場合、管理者は Cisco IPS SSP の方にユーザトラフィックを送信するのに使用する Cisco ASA のモジュラ 政策の枠組 （ MPF ）設定を取除くことができます。 この変更によりすべてのユーザトラフィックは Cisco IPS SSP モジュール インスペクションをバイパスし、パススルーにそれに Cisco ASA を与えます。

次の例に Cisco ASA ファイアウォールからの Cisco IPS ソフトウエアモジュールに Webトラフィックのリダイレクトをディセーブルにする方法を示されています:

```
ASA(config)# class-map ips_traffic
ASA(config-cmap)# match any
ASA(config)# policy-map ips_traffic_policy
ASA(config-pmap)# class ips_traffic
ASA(config-pmap-c)# no ips inline|promiscious
```

注: IPS バイパスを故障する **開いた**コマンドで設定してまたは故障する **終わりは** Cisco ASA のための Cisco IPS ソフトウエアモジュールに効果をもたらしません。

IPS が、軽減のように、混合モードで断片化したトラフィック IPS 処理のために無効である場合もあれば動作すれば。

次の例に Cisco IPS ソフトウエアモジュールの断片化したトラフィックをディセーブルにする方法を示されています:

```
sensor# conf t
sensor(config)# ser sig sig0
sensor(config-sig)# sig 1200 0
sensor(config-sig-sig)# engine normalizer
sensor(config-sig-sig-nor)# edit-default-sigs-only default-signatures-only
sensor(config-sig-sig-nor-def)# specify-max-fragments yes
sensor(config-sig-sig-nor-def-yes)# max-fragments 0
sensor(config-sig-sig-nor-def-yes)# exit
sensor(config-sig-sig-nor-def)# exit
sensor(config-sig-sig-nor)# exit
sensor(config-sig-sig)# exit
sensor(config-sig)# exit Apply Changes?[yes]: yes
```

この変更は Cisco IPS ソフトウエアモジュール リロードを必要とします。

注: この変更によりすべての非 TCP フラグメントは uninspected 渡します。

また、断片化したトラフィックは Cisco ASA ファイアウォールで拒否することができます。 これにより Cisco ASA ファイアウォールはインターフェイスのフラグメントを受け入れます。 その結果、Cisco ASA はインスペクション用の Cisco IPS ソフトウエアモジュールにフラグメントを送りません。

次の例に Cisco ASA ファイアウォールの断片化したトラフィックをディセーブルにする方法を示されています:

```
ASA(config)# fragment chain 1
```

注: 前述の例は Cisco すべての ASA インターフェイスのフラグメントをディセーブルにします。

Cisco IDSM-2 不正 な TCP パケット サービス拒否の脆弱性

しかしこの脆弱性のための回避策が、Cisco IDSM-2 モジュール 管理者 システムのマネージメントインターフェイスに接続することができるホスト（IP アドレス）の数を制限することを確かめる必要がありますありません。

許可されたホストの数を制限するために、管理者は **access-list コマンドを**使用する必要があります。 **no access-list コマンドが**リストからホストかネットワークを取除くのに使用する必要があります。
次の例はアクセスを完全な 192.168.1.0/24 ネットワークに取除き、IP アドレス 192.168.1.1 とホストにだけアクセスを許可するコマンドのシーケンスを示したものです:

- ホストかネットワークを許可される電流を見るのにネットワーク設定 コンフィギュレーションモードで**提示設定**コマンドを使用して下さい。 次の例は Cisco IDSM-2 が 192.168.1.0/24 ネットワークのすべてのホストを割り当てるために設定されることを示したものです

```
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>
  [...]
```

- 192.168.1.1 ホストを追加するネットワーク設定 コンフィギュレーションモードで **access-list コマンドを**、使用して下さい。 これが唯一の許可されたホスト、また Cisco IDSM-2 モジュールに接続を失うことを避けるように設定を実行している 1 時であることを確かめて下さい。

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

- 許可されたホスト リストのための 192.168.1.0/32 ネットワークを取除くネットワーク設定 コンフィギュレーションモードで **no access-list コマンドを**、使用して下さい。

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

- 許可されたホストのリストが正しいことを確認するのにネットワーク設定 コンフィギュレーションモードで**提示設定**コマンドを使用して下さい:

```
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、適用して下さい:

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

注: Cisco によって実行された 内部テストは許可されるホストの総数が 254 のホストと等しいかまたはそれ以下である場合この脆弱性が不正利用することができないこと見られた。 このアドバイザリで示される数に許可されたホストの数を減らすことができない管理者は追加的支援に関しては Cisco Technical Assistance Center に連絡する必要があります。

このアドバイザリに説明がある脆弱性のための追加軽減情報は次の位置でコンパニオンによって加えられる軽減情報（AMB）で利用できます:
http://tools.cisco.com/security/center/viewAMBAlert.x?alertId=29271

修正済みソフトウェア

Cisco は Cisco IDSM-2 不正 な TCP パケット サービス拒否の脆弱性を除いてこのアドバイザリのすべて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ました。 Cisco IDSM-2 モジュールの脆弱なバージョンを実行している顧客は利用可能 な軽減のためのこのアドバイザリの「回避策」セクションを参照する必要があります。

推奨されるリリース

次 の テーブルはこの Security Advisory に説明があるすべての脆弱性を解決する Cisco 推奨される IPS ソフトウェア リリースをリストします:

製品	推奨される
Cisco ASA 5500-X シリーズ IPS SSP ソフトウエアモジュール	7.1(7p1)E4 およびより高く
Cisco ASA 5585-X シリーズ IPS SSP ハードウエアモジュール	7.1(7)E4 およびより高く
Cisco IPS 4500 シリーズ センサー	7.1(7)E4 およびより高く
Cisco IPS 4300 シリーズ センサー	7.1(7)E4 およびより高く
Cisco IPS NME	7.0(9)E4 およびより高く
Cisco IDSM-2	利用可能 な リリース無し-利用可能 な軽減については「回」セクションを参照して下さい

次 の テーブルは該当製品のそれぞれのためのこのアドバイザリで個々の脆弱性のための修正が含まれている最初の修正済みリソースをリストします。 異なる脆弱性に別の最初の固定リリースがあるのでだけこの情報が完璧さに提供されることに注目して下さい。 リリースのための前の表を参照して下さいこのアドバイザリですべての脆弱性のための修正がある。

Cisco IPS ソフトウェア 不正 な IP パケット サービス拒否の脆弱性

次 の テーブルは該当製品のそれぞれの Cisco IPS ソフトウェア 不正 な IP パケット サービス拒

否の脆弱性のための修正済みリソースをリストします:

製品	該当するリリース	解決されたバージ
Cisco ASA 5500-X シリーズ IPS-SSP ソフトウェアおよびハードウエアモジュール	7.1(x)E4	7.1(5)E4
Cisco IPS 4500 シリーズ センサー	7.1(4)E4	7.1(6)E4
Cisco IPS 4300 シリーズ センサー	7.1(3)E4 および 7.1(4)E4	7.1(5)E4

注: Cisco IPS ソフトウェア リリース 7.1(5)E4 は不安定な状態問題によるダウンロード可能もうではないです。

Cisco IPS ソフトウェア 断片化したトラフィック サービス拒否の脆弱性

次 の テーブルは該当製品のそれぞれの Cisco IPS ソフトウェア 断片化したトラフィック サービス拒否の脆弱性のための修正済みリソースをリストします:

製品	該当するリリース	解決されたバージ
Cisco ASA 5500-X シリーズ IPS SSP ソフトウエアモジュール	7.1(4)E4 による 7.1(7)E4	7.1(7p1)E4

Cisco IPS NME 不正 な IP パケット サービス拒否の脆弱性

次 の テーブルは該当製品のそれぞれの Cisco IPS NME 不正 な IP パケット サービス拒否の脆弱性のための修正済みリソースをリストします:

製品	該当するリリース	解決されたバージ
高められる Cisco 侵入防御システム ネットワーク モジュール（IPS NME）	All	7.0(9)E4

ソフトウェアアップグレードを検討するとき、顧客は Cisco Security Advisory、応答および表記アーカイブを http://www.cisco.com/go/psirt で参照し、公開および完全なアップグレード ソリューションを判別するためにそれに続くアドバイザリを検討するように勧告されます。

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。

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

る脆弱性のエクスプロイト事例やその公表を確認していません。

Cisco IPS ソフトウェア 不正 な IP パケット サービス拒否の脆弱性、Cisco IPS NME 不正 な IP パケット サービス拒否の脆弱性および Cisco IDSM-2 不正 な TCP パケット サービス拒否の脆弱性は内部テストの間に検出されました。

Cisco IPS ソフトウェア 断片化したトラフィック サービス拒否の脆弱性はサポート ケースの解決の間に検出されました。

出典

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130717-ips

改訂履歴

リビジョン 1.0	2013-July-17	初回公開リリース

利用規約