Cisco Intrusion Prevention System（IPS；侵入防御システム）ソフトウェアの複数の脆弱性

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 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ソフトウェアの不正なIPパケットによるDoS脆弱性
- Cisco IPSソフトウェアのフラグメント化されたトラフィックにおけるDoS脆弱性
- Cisco IPS NMEにおける不正IPパケットに起因するDoS脆弱性
- Cisco IDSM-2における不正TCPパケットに起因するDoS脆弱性

Cisco IPSソフトウェアの不正なIPパケットによるサービス妨害(DoS)の脆弱性により、認証されていないリモートの攻撃者が MainAppプロセスを応答不能にする可能性があります。

Cisco IPSソフトウェアのフラグメント化トラフィックにおけるDoS脆弱性により、認証されていないリモートの攻撃者が、メモリ破損のために Analysis Engineプロセスを応答不能にしたり、該当システムのリロードを引き起こしたりする可能性があります。

Cisco IPS NMEの不正なIPパケットによるサービス妨害(DoS)の脆弱性により、認証されていないリモートの攻撃者がCisco Intrusion Prevention System Network Module Enhanced(IPS NME)のリロードを引き起こす可能性があります。

Cisco IDSM-2の不正TCPパケットによるサービス妨害の脆弱性により、認証されていないリモートの攻撃者がCisco Catalyst 6500シリーズIntrusion Detection System(IDSM-2)モジュールのカーネルを応答不能にする可能性があります。

これらの脆弱性が悪用されると、サービス拒否(DoS)状態が発生する可能性があります。

シスコは、「Cisco IDSM-2における不正なTCPパケットによるサービス妨害(DoS)の脆弱性」を除き、このアドバイザリに記載されている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提供しています。脆弱性のあるバージョンのCisco IDSM-2モジュールを実行しているお客様は、このアドバイザリの「回避策」セクションで利用可能な緩和策を参照してください。

Cisco IPSソフトウェアのフラグメント化トラフィックにおけるDoS脆弱性およびCisco IDSM-2における不正TCPパケットによるDoS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、次のリンクより確認できます。
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130717-ips

該当製品

脆弱性のある製品

Cisco IPSソフトウェアの不正なIPパケットによるDoS脆弱性

次の製品は、Cisco IPSソフトウェアの不正IPパケットに起因する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 IPSソフトウェア7.1 ~ 7.1(4)E4)
- Cisco IPSソフトウェアバージョン7.1(4)E4が稼働する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が稼働するCisco IPS 4300シリーズセンサー

注：この脆弱性の影響を受けるのは、Cisco IPSソフトウェアバージョン7.1を実行している製品だけです。Cisco IPSソフトウェアバージョン7.0以前を実行している製品は該当しません。

Cisco IPSソフトウェアのフラグメント化されたトラフィックにおけるDoS脆弱性

次の製品は、Cisco IPSソフトウェアのフラグメント化トラフィックにおけるDoS脆弱性の影響を受けます。

- Cisco IPSソフトウェアバージョン7.1(4)E4 ~ 7.1(7)E4を実行しているCisco ASA 5500-Xシリーズ(IPS SSP)ソフトウェアモジュール

注：Cisco IPSソフトウェアのフラグメント化トラフィックのDoS脆弱性は、Cisco ASA 5500-XシリーズIPS SSPソフトウェアモジュールのみに影響し、Cisco ASA 5585-X用のCisco IPS SSPハードウェアモジュールはこの脆弱性の影響を受けません。

Cisco IPS NMEにおける不正IPパケットに起因するDoS脆弱性

次の製品は、Cisco IPS NMEにおける不正IPパケットに起因するDoS脆弱性の影響を受けます。

- Cisco Intrusion Prevention System Network Module Enhanced(IPS NME)

Cisco IDSM-2における不正TCPパケットに起因するDoS脆弱性

次の製品は、Cisco IDSM-2における不正TCPパケットに起因するDoS脆弱性の影響を受けます。

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

実行中のソフトウェアバージョンの判別方法

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コマンドを発行します。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(IPS)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またはCisco IDMウィンドウの左上隅に表示される表で、ソフトウェアバージョンを確認できます。

脆弱性を含んでいないことが確認された製品

次の製品は、このアドバイザリに記載された脆弱性の影響を受けません。

- Cisco IOS IPS
- Cisco IPS 4200 シリーズ センサー
- Cisco Intrusion Prevention System Advanced Integration Module(IPS AIM)
- Cisco ASA 5500シリーズ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)

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ソフトウェアの不正なIPパケットによるDoS脆弱性

Cisco IPSは、ネットワークベースの脅威防御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、設定の読み取り、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。

MainAppプロセスの詳細については、製品コンフィギュレーションガイドの「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#v

IPスタックの脆弱性により、認証されていないリモートの攻撃者が MainAppプロセスを応答不能にする可能性があります。Cisco IPSセンサーがアラート通知、イベントストア管理、センサー認証などの重要なタスクを実行できないため、サービス拒否(DoS)状態が発生します。また、MainAppプロセスが応答しない間は、Cisco IPS Webサーバも使用できなくなります。また、この一般的なシステム障害が原因で、 Analysis Engineなどの他のプロセスが正しく動作しない場合があります。この脆弱性は、該当システムの管理インターフェイスからの不正なIPパケットの不適切な処理に起因します。攻撃者は、不正なIPパケットを管理インターフェ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。

この脆弱性は、管理インターフェイス宛てのIPv4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によって、この脆弱性が引き起こされることはありません。Cisco IPSが混合モードで設定されている場合、 shunや rate-limitなどのMainApp処理を必要とする緩和アクションが使用できない場合があります。Cisco IPSがインラインモードで設定されている場合、 Analysis Engineプロセスが正しく機能していない可能性があるため、センサーがインスペクションと緩和アクションを正しく実行しない可能性があります。

この脆弱性は、Cisco Bug ID CSCtx18596(登録ユーザ専用)およびCommon Vulnerabilities and Exposures(CVE)ID CVE-2013-1243で文書化されています。

Cisco IPSソフトウェアのフラグメント化されたトラフィックにおけるDoS脆弱性

Cisco IPS SSPは、Cisco ASA 5500-Xシリーズで実行される統合モジュールです。このモジュールは、Cisco ASA 5585-Xのハードウェアに導入することも、Cisco ASA 5512-X、Cisco ASA 5515-X、Cisco ASA 5525-X、Cisco ASA 5545-X、およびCisco ASA 5555-Xシリーズの統合ソフトウェアモジュールとして導入することもできます。

ASA 5500-X IPS SSPで実行されているCisco IPSソフトウェアは、Cisco ASAから受信するトラ

フィックのみを処理します。特定のトラフィックをCisco IPSソフトウェアにリダイレクトするには、Cisco ASAにモジュラポリシーフレームワーク(MPF)を設定する必要があります。

フラグメント化されたトラフィックを処理するコードの実装における脆弱性により、認証されていないリモートの攻撃者が Analysis Engineプロセスを応答不能にしたり、該当システム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、検査と処理のためにCisco ASAデータプレーンからCisco IPSプロセッサに送信されるフラグメント化IP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IPパケットと他のIPパケットの組み合わせを該当システム経由で送信することで、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、攻撃者は該当システムのリロードを引き起こしたり、 Analysis Engineプロセスが応答しなくなる可能性があります。 Analysis Engineプロセスが応答しない場合、影響を受けるシステムはトラフィックを処理しないため、そのトラフィックはドロップされます。また、該当するバージョンのソフトウェアを実行するCisco IPS SSPソフトウェアモジュールを搭載したCisco ASAがハイアベイラビリティモード(HA)に設定されている場合、Cisco IPS SSPがリロードするか、トラフィックの転送を停止すると、フェールオーバーイベントがトリガーされる可能性があります。

この脆弱性は、該当システムを通過するIPv4およびIPv6フラグメント化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ソフトウェアモジュールの管理IPアドレス宛てのトラフィックは、この脆弱性を引き起こしません。

注：この脆弱性の影響を受けるのは、Cisco ASA 5500-XシリーズIPS SSPソフトウェアモジュールだけです。Cisco ASA5585-XシリーズでサポートされているCisco IPS SSPハードウェアモジュールは、この脆弱性の影響を受けません。

この脆弱性は、Cisco Bug ID CSCue51272(登録ユーザ専用)として文書化され、CVE IDとしてCVE-2013-1218が割り当てられています。

Cisco IPS NMEにおける不正IPパケットに起因するDoS脆弱性

メモリ割り当てコードに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システム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、該当システムの管理インターフェイスで不正なIPパケットが受信されたときに、メモリ割り当てが適切に処理されないことに起因します。攻撃者は、不正なIPパケットを管理IPアドレ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。

この脆弱性は、管理インターフェイス宛てのIPv4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によって、この脆弱性が引き起こされることはありません。

この脆弱性の影響を受けるのは、Cisco IPS NMEで稼働しているCisco IPSソフトウェアだけです

。

この脆弱性は、Cisco Bug ID CSCua61977(登録ユーザ専用)として文書化され、CVE IDとしてCVE-2013-3410が割り当てられています。

Cisco IDSM-2における不正TCPパケットに起因するDoS脆弱性

IDSM-2ドライバの脆弱性により、認証されていないリモートの攻撃者がシステムカーネルを応答不能にする可能性があります。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、トラフィック検査など、いくつかの重要なタスクを実行できないため、サービス拒否(DoS)状態が発生します。Cisco IPS Webサーバも使用できなくなります。

この脆弱性は、該当システムの管理インターフェイスからの不正なTCPパケットの不適切な処理に起因します。攻撃者は、不正なIPパケットを管理インターフェ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ためにTCP 3ウェイハンドシェイクは必要ありません。システムの機能を復元するには、ハードシステムリブートが必要です。

この脆弱性は、管理インターフェイス宛てのIPv4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によって、この脆弱性が引き起こされることはありません。

この脆弱性は、Cisco IDSM-2モジュールで実行されているCisco IPSソフトウェアにのみ影響します。

この脆弱性は、Cisco Bug ID CSCuh27460(登録ユーザ専用)として文書化され、CVE IDとしてCVE-2013-3411が割り当てられています。

回避策

Cisco IPSソフトウェアにおける不正IPパケットに起因するDoS脆弱性およびCisco IPS NMEにおける不正IPパケットに起因するDoS脆弱性

この脆弱性を軽減する回避策はありません。

Cisco IPSソフトウェアのフラグメント化されたトラフィックにおけるDoS脆弱性

この脆弱性のエクスプロイトがトラフィックの中断を引き起こしている場合、管理者は、ユーザトラフィックをCisco IPS SSPに向けるために使用するCisco ASAのモジュラポリシーフレームワーク(MPF)の設定を削除できます。この変更により、すべてのユーザトラフィックがCisco IPS SSPモジュールインスペクションをバイパスし、Cisco ASAを通過できるようになります。

次の例は、Cisco ASAファイアウォールからCisco IPSソフトウェアモジュールへのWebトラフィ

ックのリダイレクトを無効にする方法を示しています。

```
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：コマンド fail-openまたは fail-closeを使用してIPSバイパスを設定しても、Cisco ASAのCisco IPSソフトウェアモジュールには影響しません。

IPSが混合モードで動作している場合は、その緩和策として、フラグメント化されたトラフィックをIPS処理に対して無効にすることができます。

次の例は、Cisco IPSソフトウェアモジュールでフラグメント化されたトラフィックを無効にする方法を示しています。

```
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
```

この変更には、Cisco IPSソフトウェアモジュールのリロードが必要です。

注：この変更により、すべての非TCPフラグメントが検査されずに通過することになります。

また、フラグメント化されたトラフィックをCisco ASAファイアウォールで許可しないこともできます。これにより、Cisco ASAファイアウォールはインターフェイス上のフラグメントを受け入れなくなります。その結果、Cisco ASAは検査のためにCisco IPSソフトウェアモジュールにフラグメントを送信しません。

次の例は、Cisco ASAファイアウォールでフラグメント化されたトラフィックを無効にする方法を示しています。

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

注：前の例では、すべてのCisco ASAインターフェイスでフラグメントを無効にしています。

Cisco IDSM-2における不正TCPパケットに起因するDoS脆弱性

この脆弱性に対する回避策はありませんが、Cisco IDSM-2モジュール管理者は、システムの管理インターフェイスへの接続が許可されるホスト（IPアドレス）の数を制限する必要があります。

許可するホストの数を制限するには、管理者が access-listコマンドを使用する必要があります。no access-listコマンドは、リストからすべてのホストまたはネットワークを削除するために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を削除し、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一連のコマンドを示しています。

- 現在許可されているホストまたはネットワークを確認するには、ネットワーク設定設定モードでshow settingsコマンドを使用します。次の例は、Cisco IDSM-2が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>
      [...]
```

- 192.168.1.1ホストを追加するには、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コマンドを使用します。これが唯一の許可ホストである場合は、Cisco IDSM-2モジュールへの接続が失われないように、設定を実行するのもこのホストであることを確認してください。

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

- 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、許可されるホストリストから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
```

- 許可されるホストのリストが正しいことを確認するには、ネットワーク設定設定モードでshow settingコマンドを使用します。

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

- 設定を終了して適用します。

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

注：シスコが実施した内部テストでは、許可されたホストの総数が254台以下の場合には、この脆弱性はエクスプロイトできないことが示されています。許可されるホストの数をこのアドバイザリで示されている数に減らすことができない管理者は、Cisco Technical Assistance Center(TAC)に連絡して追加サポートを受ける必要があります。

このアドバイザリに記載されている脆弱性に関する追加の緩和策については、このアドバイザリに関連するApplied Mitigation Bulletin(AMB)を参照してください。AMBは次の場所にあります。
https://sec.cloudapps.cisco.com/security/center/viewAMBAlert.x?alertId=29271

修正済みソフトウェア

シスコは、「Cisco IDSM-2における不正なTCPパケットによるサービス妨害(DoS)の脆弱性」を除き、このアドバイザリに記載されている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提供しています。脆弱性のあるバージョンのCisco IDSM-2モジュールを実行しているお客様は、このアドバイザリの「回避策」セクションで利用可能な緩和策を参照してください。

推奨リリース

次の表に、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修正する推奨Cisco IPSソフトウェアリリースを示します。

製品	推奨
Cisco ASA 5500-XシリーズIPS	7.1(7p1)E4以降

SSPソフトウェアモジュール	
Cisco ASA 5585-XシリーズIPS SSPハードウェアモジュール	7.1(7)E4以降
Cisco IPS 4500 シリーズ センサー	7.1(7)E4以降
Cisco IPS 4300 シリーズ センサー	7.1(7)E4以降
Cisco IPS NME	7.0(9)E4以降
Cisco IDSM-2	使用可能なリリースがありません。使用可能な緩和策については、「回避策」セクションを参照してください。

次の表に、影響を受ける各製品に関するこのアドバイザリに記載された個々の脆弱性に対する修正を含む最初の修正済みリリースを示します。この情報は、脆弱性によって最初の修正リリースが異なるため、完全を期して提供されています。このアドバイザリに記載されているすべての脆弱性に対する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。

Cisco IPSソフトウェアの不正なIPパケットによるDoS脆弱性

次の表に、Cisco IPSソフトウェアの不正IPパケットに関するDoS脆弱性に対する修正済みリリースを、該当製品ごとに示します。

製品	該当するリリース	解決されたバージョン
Cisco ASA 5500-XシリーズIPS-SSPソフトウェアおよびハードウェアモジュール	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、不安定な問題が原因でダウンロードできなくなりました。

Cisco IPSソフトウェアのフラグメント化されたトラフィックにおけるDoS脆弱性

次の表に、Cisco IPSソフトウェアのフラグメント化トラフィックにおけるDoS脆弱性に対する修正済みリリースを、該当製品ごとに示します。

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

Cisco IPS NMEにおける不正IPパケットに起因するDoS脆弱性

次の表に、Cisco IPS NMEにおける不正IPパケットに関するDoS脆弱性の修正済みリリースを、該当製品ごとに示します。

製品	該当するリリース	解決されたバージョン
Cisco Intrusion Prevention System Network Module Enhanced(IPS NME)	すべて	7.0(9)E4

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。

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。

Cisco IPSソフトウェアの不正なIPパケットに起因するDoS脆弱性、Cisco IPS NMEの不正なIPパケットに起因するDoS脆弱性、およびCisco IDSM-2の不正なTCPパケットに起因するDoS脆弱性は、シスコの社内テストによって発見されたものです。

Cisco IPSソフトウェアのフラグメント化トラフィックにおけるDoS脆弱性は、サポートケースの解決中に発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130717-ips

改訂履歴

リビジョン 1.0	2013年7月17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。