Cisco IPSソフトウェアの複数の脆弱性

アドバイザリーID : cisco-sa-20140219-ips
初公開日 : 2014-02-19 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 : CSCui91266 CSCui67394 CSCuh94944

CVE-2014-0718
CVE-2014-0719
CVE-2014-0720

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 Analysis EngineのDoS脆弱性
- Cisco IPS Control-Plane MainAppのDoS脆弱性
- Cisco IPSのジャンボフレームにおけるdos脆弱性

Cisco IPS Analysis Engineのサービス拒否の脆弱性およびCisco IPSのジャンボフレームのサービス拒否の脆弱性により、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、クラッシュさせたりする可能性があります。この場合、Cisco IPSはトラフィックの検査を停止します。

Cisco IPS Control-Plane MainAppのDoS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し、アラート通知、イベントストア管理、センサー認証などの複数のタスクの実行を妨害する可能性があります。また、 MainAppプロセスが応答しない間はCisco IPS Webサーバも使用できず、 Analysis Engineプロセス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。

シスコはこれら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。一部の脆弱性に対しては回避策があります。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-20140219-ips

該当製品

脆弱性のある製品

Cisco IPS Analysis EngineのDoS脆弱性

次の製品は、Cisco IPS Analysis Engine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。

この脆弱性は、produce-verbose-alertアクションが有効になっているシグニチャが設定されているCisco IPSソフトウェア、またはこのアクションを追加するよう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にのみ影響を与えます。

produce-verbose-alertオプションがアクティブなシグニチャまたは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rules0イベントアクションルールポリシーを示しています。

```
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、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の順に選択して、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、アクティブなシグニチャおよびEAOルールではデフォルトで有効になっていません。

Cisco IPS Control-Plane MainAppのDoS脆弱性

次の製品は、Cisco IPS Control-Plane 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用の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リリースのマイルストーンが終了しています。代替製品については、シスコの担当者にお問い合わせください。

Cisco IPSのジャンボフレームにおけるDoS脆弱性

次の製品は、Cisco IPS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

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、アプリケーションの開始と停止、認証サービスなど、複数の重要なタスクを実行します。一方、分析エンジンプロセスは、センサー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プロセスについての詳細は、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

Cisco IPS Analysis Engine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の攻撃者がAnalysis Engineプロセスを応答不能にする可能性があります。

この脆弱性は、 produce-verbose-alertアクションが有効な場合に、分析エンジンプロセスによってフラグメント化されたパケットが適切に処理されないことに起因します。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。脆弱性を引き起こすには、攻撃者は produce-verbose-alertアクションを含むシグニチャを起動するか、イベントアクションオーバーライドとして produce-verbose-alertが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、攻撃者はAnalysis Engineプロセスを応答不能にする可能性があります。これにより、該当するシステムでトラフィックの検査が停止します。

この脆弱性は、該当システムを通過するIPバージョン4(IPv4)およびIPバージョン6(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。

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 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 MainAppプロセスを応答不能にす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る不正な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、管理インターフェイスのIPアドレスのTCPポート7000に巧妙に細工されたTCPパケットを送信することで、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、攻撃者は 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、管理インターフェイスのIPアドレスのTCPポート7000宛ての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プロセスが正しく動作し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 ASA 5500シリーズおよびCisco ASA 5500-Xシリーズのハードウェアおよびソフトウェア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 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における 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の攻撃者がAnalysis Engineプロセスを応答不能にする可能性があります。

この脆弱性は、高レートで送信されるジャンボフレームの不適切な処理に起因します。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、攻撃者はAnalysis Engineプロセスを応答不能にする可能性があります。これにより、該当するシステムでトラフィックの検査が停止します。

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る可能性があります。Cisco IPS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。

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。

回避策

Cisco IPS Analysis Engineのサービス拒否の脆弱性を回避するには、 produce-verbose-alertアクションを無効にします。

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判別するか、または produce-verbose-alertオプションがEAOとして有効になっているシグニチャを判別します。

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、変更が必要な各シグニチャのイベントアクションを produce-verbose-alertアクションの代わりに produce-alertを使用して変更することで、値を変更できます。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)#
```

あるいは、管理者はCisco Intrusion Prevention System(IPS)Device Manager(IDM)を使用してCisco IPSに接続し、 Configuration > Policies > Signature Definitions > -Sig-Definition-Name- > Active Signaturesに移動し、Filter: Action Produce Verbose Alertを使用してフィルタリングを行い、 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できます。

各シグニチャを右クリックし、 Edit Actionを選択します。パネルで Produce Verbose Alertチェックボックスのチェックマークを外し、 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することで無効にできます。

次の例は、 rules0イベントアクションルールポリシーで設定されている produce-verbose-alertによる上書き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 MainAppのDoS脆弱性に対する回避策はありませんが、許可するホストの数を制限することで、この脆弱性の発現を減らすことができます。

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>
      [...]
```

- 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、192.168.1.1ホストを追加します。

注：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、コンフィギュレーションコマンド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
```

- 許可された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 settings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]:
```

Cisco IPSのジャンボフレームの DoS脆弱性に対する回避策はありません。

ネットワーク内の Cisco デバイスに導入でき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 Cisco 適用インテリジェンス (https://sec.cloudapps.cisco.com/security/center/viewAMBAlert.x?alertId=32605) を参照してください。

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。

次の表に、各脆弱性と各メジャーリリースバージョンの最初の修正リリースをまとめます。最後の行に、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解決する推奨リリースに関する情報を示します。

	6.x	7.0	7.1	7.2	7.3
Cisco IPS Analysis EngineのDoS脆弱性 – CSCui91266	Not affected	Not affected	7.1(8)E4[1]	7.2(2)E4	Not affected
Cisco IPS Control-Plane MainAppのDoS脆弱性 – CSCui67394	該当、7.1以降に移行[2]	該当する、7.1以降に移行	7.1(8p2)E4	7.2(2)E4	Not affected
Cisco IPSのジャンボフレームにおけるDoS脆弱性 – CSCuh94944	Not affected	Not affected	7.1(8)E4	7.2(2)E4	Not affected
推奨リリース	該当する、7.1以降に移行	該当する、7.1以降に移行	7.1(8p2)E4以降	7.2(2)E4以降	Not affected

[1]この脆弱性は、7.1(4)E4より前の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)は、Cisco IPSソフトウェアバージョン6.2以前のみをサポートしています。Cisco ASA 5505用の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リリースのマイルストーンが終了しています。

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）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とその公表は確認しておりません。

Cisco IPS Analysis Engineのサービス拒否の脆弱性とCisco IPS Control-PlaneのMainAppのサービス拒否の脆弱性は、カスタマーサービスリクエストの解決中に発見されました。Cisco IPSのジャンボフレームにおけるの脆弱性は、シスコ内部でのテストによって発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140219-ips

改訂履歴

リビジョン 1.0	2014年2月19日	初版リリース

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。