Cisco IOSソフトウェア IPS およびゾーンはファイアウォール脆弱性を基づかせていました

High	**アドバイザリーID :** cisco-sa-20110928-zbfw **初公開日 :** 2011-09-28 16:00 **最終更新日 :** 2012-09-21 19:24 **バージョン 1.2 :** Final **CVSSスコア :** 7.8 **回避策 :** Yes **Cisco バグ ID :** CSCto68554 , CSCti79848	CVE-2011-3281 CVE-2011-3273

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 IOSソフトウェアは Cisco IOS 侵入防御システム（IPS）および Cisco IOS ゾーン ベースのファイアウォール特性に関する 2 脆弱性が含まれています。 これらの脆弱性は次のとおりです:

- Cisco IOSソフトウェアのメモリリーク
- 特別に 巧妙に細工された HTTP パケットを処理した場合 Cisco IOSソフトウェア Denial of Service（DoS/DDoS）

シスコはこれらの脆弱性に対処するソフトウェア アップデートを提供しています。これらの脆弱性を軽減する回避策は利用できません。このアドバイザリは 928-zbfw で掲示されます。 **注:** 2011 年 9月 28 日、Cisco IOSソフトウェア Security Advisory によって組み込まれる書は 10 Cisco Security Advisory が含まれています。 アドバイザリの 9 つは Cisco IOSソフトウェアの脆弱性に対処し、1 つのアドバイザリは Cisco Unified Communications Manager の脆弱性に対処します。 各アドバイザリは正しい 2011 年 9 月のすべての脆弱性はパブリケーションを組み込んだことアドバイザリ、また Cisco IOS ソフトウェア リリースで詳述される脆弱性を解決する Cisco IOS ソフトウェア リリースをリストします。"Cisco Event Response: 半年ごと Cisco IOSソフトウェア Security Advisory は次のリンクのパブリケーションを」組み込みました :http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep11.html

該当製品

修正済みソフトウェア

Cisco IOSソフトウェアの脆弱なバージョンを実行する Cisco IOSデバイスは Cisco IOS IPS お

よび Cisco IOS ゾーン ベースのファイアウォールの 2 脆弱性から影響を受けます。 2 脆弱性は互いの依存しないです。 影響を受けたコンフィギュレーションを確認する詳細は下記に提供されます。

- Cisco IOSソフトウェアのメモリリーク
  Cisco IOS IPS か Cisco IOS ゾーン ベースのファイアウォール設定されるデバイスはデバイスを通る新しいセッション作成フローの高い率の下で（または両方）のために、メモリリークを経験するかもしれません。
  デバイスが Cisco IOS IPS で設定されたかどうか確認するために、デバイスにログイン し、**提示 IP IPS インターフェイス** CLI コマンドを発行して下さい。 出力が着信 または 発信 方向 セットで IPS ルールにどちらかを示したもので場合、デバイスは脆弱です。 この例は受信方向で、インターフェイス 0/0 の IPS ルール セットのデバイスをギガビット イーサネット（802.3z）示したものです:

```
Router#show ip ips interfaces
    Interface Configuration
      Interface GigabitEthernet0/0
        Inbound IPS rule is example_ips_rule
        Outgoing IPS rule is not set
```

  Router#Cisco IOS IPS のために設定されないデバイスはブランク 行を戻します。 次の例は Cisco IOS が IPS 設定されないデバイスを示したものです:

```
Router#show ip ips interfaces

Router#
```

  デバイスがゾーン ベースのファイアウォールで設定されるかどうか判別するために、デバイスにログイン し、**show zone セキュリティ** CLI コマンドを発行して下さい。 出力が zone name の下でメンバー インターフェイスを示したもので場合、デバイスは脆弱です。 この例は、GigabitEthernet0/0 および GigabitEthernet0/1 両方でゾーン ベースのファイアウォール ルールが設定されているデバイスを示したものです

```
Router#show zone security
zone self
  Description: System defined zone


zone inside
  Description: *** Inside Network ***
  Member Interfaces:
    GigabitEthernet0/0


zone outside
  Description: *** Outside Network ***
  Member Interfaces:
    GigabitEthernet0/1
```

  Router#**注:** デバイスは実行された パケット点検の種類に関係なくゾーン ベースのファイアウォールと脆弱もし設定するなら、です。
- 特別に 巧妙に細工された HTTP パケットを処理した場合 Cisco IOSソフトウェア Denial of Service（DoS/DDoS）
  デバイスは次の状況のもとで脆弱もし設定するならです:
  - HTTP レイヤ7 アプリケーション コントロールおよびインスペクションおよび Cisco IOS

IPS は有効に なります。
-一致との HTTP レイヤ7 アプリケーション コントロールおよびインスペクションは HTTP クラスマップの引数 regex パラメータを要求します。 この設定は Cisco IOS IPS が有効に なるかどうかそれにもかかわらず影響を受けます。

デバイスは脆弱 で はない下他のコンフィギュレーションではないです。 この脆弱性による異なる構成および影響の要約は下記のように提供されます:

次の例は HTTP レイヤ7 アプリケーション コントロールでおよびインスペクション設定される影響を受けた有効に なる デバイスおよび Cisco IOS IPS 示したものです:!

```
ip ips name myips
!
ip ips signature-category
  category all
   retired true
  category ios_ips basic
   retired false
!
!
class-map type inspect match-any layer4-classmap
 match protocol http
!
class-map type inspect http match-any layer7-classmap
  match  request arg length gt 15
!
!
policy-map type inspect http layer7-policymap
 class type inspect http layer7-classmap
  reset
  log
policy-map type inspect layer4-policymap
 class type inspect layer4-classmap
  inspect
  service-policy http layer7-policymap
 class class-default
  drop
!
zone security inside
 description ** Inside Network **
zone security outside
 description ** Outside Network **
zone-pair security in2out source inside destination outside
 description ** Zone Pair - inside to outside **
 service-policy type inspect layer4-policymap
!
!
interface GigabitEthernet0/0
 ip address 192.168.0.6 255.255.255.0
 ip ips myips in
 zone-member security inside
!
interface GigabitEthernet0/1
 ip address 192.168.1.1 255.255.255.0
 zone-member security outside
```

!次の例は HTTP クラスマップの**一致要求引数 regex** パラメータの HTTP レイヤ7 アプリケーション コントロールおよびインスペクションで設定される影響を受けたデバイスを示

したものです:

```
!
parameter-map type regex example
 pattern [^\x00-\x80]
!
class-map type inspect match-any layer4-classmap
 match protocol http
!
class-map type inspect http match-any layer7-classmap
 match  request arg regex example
!
!
policy-map type inspect http layer7-policymap
 class type inspect http layer7-classmap
  reset
  log
policy-map type inspect layer4-policymap
 class type inspect layer4-classmap
  inspect
  service-policy http layer7-policymap
 class class-default
  drop
!
zone security inside
 description ** Inside Network **
zone security outside
 description ** Outside Network **
zone-pair security in2out source inside destination outside
 description ** Zone Pair - inside to outside **
 service-policy type inspect layer4-policymap
!
interface GigabitEthernet0/0
 ip address 192.168.0.6 255.255.255.0
 zone-member security inside
!
interface GigabitEthernet0/1
 ip address 192.168.1.1 255.255.255.0
 zone-member security outside
!
```

Cisco 製品で稼働している Cisco IOS ソフトウェア リリースを確認するには、機器にログインし show version コマンドを実行してシステムバナーを表示させます。 "Internetwork Operating System Software"、"Cisco IOS Software" あるいはこれらに類似するシステム バナーによってデバイスで Cisco IOS ソフトウェアが稼働していることを確認できます。 その後ろにイメージ名が括弧の間に表示され、続いて "Version" と Cisco IOS ソフトウエア リリース名が表示されます。 他の Cisco 機器では、 show version コマンドがない場合や、表示が異なる場合があります。次の例は C3900-UNIVERSALK9-M のインストール済みイメージ名前と Cisco IOS ソフトウェア リリース 15.0(1)M1 を実行している Cisco製品を指定したものです:

```
Router> show version
Cisco IOS Software, C3900 Software (C3900-UNIVERSALK9-M), Version 15.0(1)M1, RELEASE SOFTWARE
(fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2009 by Cisco Systems, Inc.
Compiled Wed 02-Dec-09 17:17 by prod_rel_team

!--- output truncated
```

Cisco IOS ソフトウェア リリース 命名規則についてのその他の情報は http://www.cisco.com/web/about/security/intelligence/ios-ref.html で白書 *Cisco IOS および NX-OS ソフトウェア レファレンスガイド*で利用できます。

脆弱性を含んでいないことが確認された製品

以下の製品は確認された脆弱です:

- Cisco PIX 500 シリーズ ファイアウォール
- Cisco ASA 5500 シリーズ 適応型セキュリティ アプライアンス（ASA）ソフトウェア
- Catalyst 6500 スイッチ用の Firewall Services Module （FWSM）および 7600 シリーズ ルータ
- Cisco XR 12000 シリーズ ルータのマルチサービス ブレード（MSB）の仮想 な ファイアウォール（VFW）アプリケーション
- Cisco ACE アプリケーション コントロール エンジン モジュール
- レガシー Cisco IOS Firewall サポートで設定される Cisco IOSデバイス
- Cisco IOS XR ソフトウェア
- Cisco IOS XE ソフトウェア
- Cisco IPS アプライアンス
- Cisco Catalyst 6500 シリーズ ASA サービス モジュール
- コンテンツは基づかせていましたアクセスコントロール（CBAC）を

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。

改訂履歴

リビジョン 1.2	2011-September-30	更新済 Cisco IOSソフトウェア 表によって組み込まれる書第 1 固定情報。
リビジョン 1.1	2011-September-28	リリース 15.0S および 15.1S のための固定 Cisco IOSソフトウェア 表の追加された抜けた 情報。
リビジョン 1.0	2011-September-28	初回公開リリース

利用規約