Cisco Content Services ゲートウェイ脆弱性

High	**アドバイザリーID :** cisco-sa-20110126-csg2 **初公開日 :** 2011-01-26 16:00 **バージョン 1.0 :** Final **CVSSスコア :** 7.8 **回避策 :** Yes **Cisco バグ ID :**	CVE-2011-0348 CVE-2011-0349 CVE-2011-0350

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 Content Services ゲートウェイで存在 する サービス ポリシー バイパス の 脆弱性- Cisco Service and Application Module for IP （ サーミ語 ）で動作する第 二 世代（CSG2）。 ある特定のコンフィギュレーションの下でこの脆弱性は割り当てる可能性があります:

- 普通エンド カスタマーへ満たされないでアクセスされるべき請求ポリシーを一致する サイトにアクセスする顧客
- 設定された制約事項ポリシーに基づいて普通否定されるサイトにアクセスする顧客

さらに、Cisco CSG2 の Cisco IOS ソフトウェア リリース 12.4(24)MD1 はトラフィックは CSG2 を通ることを防ぐサービス拒否状態を作成するのにリモートの、非認証攻撃者によって不正利用することができる 2 脆弱性が含まれています。 これらの脆弱性は単一 コンテンツサービスだけ Cisco CSG2 でアクティブであるように要求し、巧妙に細工された TCP パケットによって不正利用することができます。 これらの脆弱性の不正利用するために 3方向ハンドシェイクが必要となりません。

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 126-csg2 で掲示されます。

該当製品

修正済みソフトウェア

Cisco CSG2 で動作している Cisco IOSソフトウェアのバージョンを判別するために、どんな

モジュールおよびサブモジュールがシステムでインストールされているか識別するために Cisco CSG2 モジュールがインストールされているスイッチの Cisco IOSソフトウェアからの**" show module " コマンドを**発行して下さい。

Cisco CSG2 は Cisco Service and Application Module for IP（サーミ語）カードで動作し、スロット 2 の次の例で WS-SVC-SAMI-BB-K9 識別によって識別されます:

```
C7600#show module
Mod Ports Card Type                                Model              Serial No.
--- ----- ---------------------------------------- ------------------ -----------
  1    2  Supervisor Engine 720 (Active)         WS-SUP720-3BXL     JAF1226ARQS
  2    1  SAMI Module (csgk9)                     WS-SVC-SAMI-BB-K9  SAD113906P1
  4   48  CEF720 48 port 10/100/1000mb Ethernet  WS-X6748-GE-TX     SAL1127T6XY

Mod MAC addresses                       Hw    Fw           Sw           Status
--- ----------------------------------- ------ ------------ ------------ -------
  1  001e.be6e.a018 to 001e.be6e.a01b   5.6   8.5(2)       12.2(33)SRC5 Ok
  2  001d.45f8.f3dc to 001d.45f8.f3e3   2.1   8.7(0.22)FW1 12.4(2010040 Ok
  4  001c.587a.ef20 to 001c.587a.ef4f   2.6   12.2(14r)S5  12.2(33)SRC5 Ok

Mod  Sub-Module                  Model              Serial       Hw     Status
---- --------------------------- ------------------ ----------- ------- -------
  1  Policy Feature Card 3       WS-F6K-PFC3BXL     JAF1226BNQM  1.8    Ok
  1  MSFC3 Daughterboard         WS-SUP720          JAF1226BNMC  3.1    Ok
  2  SAMI Daughterboard 1        SAMI-DC-BB         SAD114400L9  1.1    Other
  2  SAMI Daughterboard 2        SAMI-DC-BB         SAD114207FU  1.1    Other
  4  Centralized Forwarding Card WS-F6700-CFC       SAL1029VGFK  2.0    Ok

Mod  Online Diag Status
---- -------------------
  1  Pass
  2  Pass
  4  Pass
C7600#
```

正しいスロットを見つけた後、それぞれ Cisco CSG2 にコンソール接続を開くために**「セッション スロット <module number> プロセッサ <3-9>"** コマンドを発行して下さい。 Cisco CSG2 に接続されて、**" show version " コマンドを**実行して下さい:

次の例は Cisco CSG2 がソフトウェア リリース 12.4(24)MD1 を実行していることを示したものです:

```
CSG2#show version
Cisco IOS Software, SAMI Software (SAMI-CSGK9-M), Version 12.4(24)MD1, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2010 by Cisco Systems, Inc.
Compiled Wed 07-Apr-10 09:50 by prod_rel_team


--- output truncated ---
```

脆弱性を含んでいないことが確認された製品

Cisco Content Services Gateway - 第 1 世代（CSG）はこれらの脆弱性から影響を受けません。

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 1.0	2011-January-26	初回公開リリース

利用規約

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も示唆するものではありません。 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、シスコは本ドキュメントの内容を予告なしに変更したり、更新したりする権利を有します。
本アドバイザリの記述内容に関して情報配信の URL を省略し、単独の転載や意訳を施した場合、当社が管理した情報とは見なされません。そうした情報は、事実誤認を引き起こしたり、重要な情報が欠落していたりする可能性があります。 このドキュメントの情報は、シスコ製品のエンドユーザを対象としています。