Cisco Content Services GatewayのDoS脆弱性

severity

アドバイザリーID : cisco-sa-20110706-csg

初公開日 : 2011-07-06 16:00

バージョン 1.0 : Final

回避策 : No Workarounds available

Cisco バグ ID :

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 Service and Application Module for IP(SAMI)上で動作するCisco Content Services Gateway - Second Generation(CSS)には、サービス拒否(DoS)の脆弱性が存在します。認証されていないリモートの攻撃者は、巧妙に細工された一連のICMPパケットを該当デバ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。この脆弱性が悪用されると、デバイスがリロードされる可能性があります。

該当デバイス宛てのICMPトラフィックをブロックする以外に、この脆弱性の不正利用を軽減する回避策はありません。

このアドバイザリは、https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110706-csg で公開されています。

該当製品

脆弱性のある製品

このアドバイザリの「ソフトウェアバージョンと修正」セクションに示されているように、最初の修正リリースより前の第2世代のContent Services Gateway用Cisco IOSソフトウェアのすべてのバージョンが影響を受けます。

Cisco CSGソフトウェアバージョンの確認

Cisco CSG2で実行されているCisco IOSソフトウェアのバージョンを確認するには、Cisco CSG2モジュールがインストールされているスイッチでCisco IOSソフトウェアから**show module**コマンドを発行して、システムにインストールされているモジュールとサブモジュール

を特定します。

Cisco Content Services Gateway：第2世代はCisco Service and Application Module for IP(SAMI)カード上で動作し、WS-SVC-SAMI-BB-K9の識別機能によってスロット2で次の例のように識別されます。

```
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ら、「**session slot <module number> processor <3-9>**」コマンドを発行して、対応するCiscoコンテンツサービスゲートウェイ：第2世代へのコンソール接続を開きます。例：**session slot 2 processor 3**。3は、CSG2の制御プロセッサ(CP)番号です。Cisco Content Services Gateway: Second Generationを設定または監視する際は、必ずCP 3にセッションします。Cisco Content Services Gateway: Second Generationに接続したら、「**show version**」コマンドを実行します。

次の例は、Cisco Content Services Gateway: Second Generation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ています。

```
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

Content Services Gateway：第1世代は、この脆弱性の影響を受けません。

注：他のSAMIベースのアプリケーションは影響を受けません。Cisco Gateway GPRS Support Node(GGSN)、Cisco Mobile Wireless Home Agent(HA)、Cisco Wireless Security Gateway(WSG)、Cisco Broadband Wireless GatewayとCisco IP Transfer Point(ITP)、およびCisco Long Term Evolution(LTE)ゲートウェイは影響を受けません。

Cisco 7600シリーズルータは、この脆弱性の影響を受けません。影響を受けるのは、Cisco CSG（第2世代）モジュールだけです。

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 Content Services Gateway：第2世代は、ディープパケットインスペクションに基づく柔軟なポリシー管理や課金などのインテリジェントなネットワーク機能と、モバイル事業者がモバイルデータネットワーク上で付加価値の高い差別化されたサービスを迅速かつ容易に提供できるようにする加入者およびアプリケーション認識機能を提供します。

Cisco Content Services GatewayにはDoSの脆弱性が存在します。第2世代では、認証されていない攻撃者が、巧妙に細工されたICMPメッセージを該当デバイスに送信することで、デバイスのリロードを引き起こす可能性があります。

注：Cisco Gateway GPRS Support Node(GGSN)、Cisco Mobile Wireless Home Agent(HA)、Cisco Wireless Security Gateway(WSG)、Cisco Broadband Wireless GatewayとCisco IP Transfer Point(ITP)、およびCisco Long Term Evolution(LTE)Gatewayは影響を受けません。

この脆弱性は、Cisco Bug ID CSCtl79577 (登録ユーザ専用)として文書化され、CVE IDとしてCVE-2011-2064が割り当てられています。

回避策

Cisco 7600ルータにインフラストラクチャアクセスコントロールリスト(iACL)を適用して、Cisco CSGのIPアドレス宛てのICMPトラフィックをブロックする以外に、この脆弱性を軽減する回避策はありません。管理者は、既存のセキュリティポリシーと設定に従って、入力アクセスポイントからネットワークに入ることを許可されたトラフィックだけを明示的に許可するか、ネットワークを通過することを許可されたトラフィックを許可することによって、iACLを構築できます。iACLによる回避策では、信頼できる送信元アドレスから攻撃が発信された場合に、これらの脆弱性に対する完全な保護を提供することはできません。

iACLポリシーは、エコー要求、エコー応答、ホスト到達不能、traceroute、packet-too-big、time-exceeded、到達不能など、不正なICMPパケットタイプが該当デバイスに送信されることを拒否します。次の例では、192.168.60.0/24が影響を受けるデバイスによって使用されるIPアドレス空

間であり、192.168.100.1にあるホストは、影響を受けるデバイスへのアクセスを必要とする信頼できる送信元と見なされます。許可されないすべてのトラフィックを拒否する前に、ルーティングおよび管理アクセスに必要なトラフィックを許可するように注意する必要があります。インフラストラクチャのアドレス レンジは、できるだけユーザおよびサービス セグメントに使用されるアドレス レンジとは別個にする必要があります。このようにアドレスを設定することで、iACLの構築と配備が容易になります。

iACLについての詳細は、『コアの保護：インフラストラクチャ保護ACL』を参照してください。

```
ip access-list extended Infrastructure-ACL-Policy

 !
  !-- Include explicit permit statements for trusted sources
  !-- that require access on the vulnerable protocol
  !

  permit icmp host 192.168.100.1 192.168.60.0 0.0.0.255 echo
  permit icmp host 192.168.100.1 192.168.60.0 0.0.0.255 echo-reply
  permit icmp host 192.168.100.1 192.168.60.0 0.0.0.255 host-unreachable
  permit icmp host 192.168.100.1 192.168.60.0 0.0.0.255 traceroute
  permit icmp host 192.168.100.1 192.168.60.0 0.0.0.255 packet-too-big
  permit icmp host 192.168.100.1 192.168.60.0 0.0.0.255 time-exceeded
  permit icmp host 192.168.100.1 192.168.60.0 0.0.0.255 unreachable

  !
  !-- The following vulnerability-specific access control entries
  !-- (ACEs) can aid in identification of attacks
  !

  deny icmp any 192.168.60.0 0.0.0.255 echo
  deny icmp any 192.168.60.0 0.0.0.255 echo-reply
  deny icmp any 192.168.60.0 0.0.0.255 host-unreachable
  deny icmp any 192.168.60.0 0.0.0.255 traceroute
  deny icmp any 192.168.60.0 0.0.0.255 packet-too-big
  deny icmp any 192.168.60.0 0.0.0.255 time-exceeded
  deny icmp any 192.168.60.0 0.0.0.255 unreachable

  !
  !-- Explicit deny ACE for traffic sent to addresses configured within
  !-- the infrastructure address space
  !

  deny ip any 192.168.60.0 0.0.0.255

!
  !-- Permit or deny all other Layer 3 and Layer 4 traffic in accordance
  !-- with existing security policies and configurations
  !
!-- Apply iACL to interfaces in the ingress direction
!

interface GigabitEthernet0/0
 ip access-group Infrastructure-ACL-Policy in
```

ネットワーク内のCiscoデバイスに適用可能な他の緩和策については、このアドバイザリに関連するCisco適用対応策速報
(https://sec.cloudapps.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-

amb-20110706-csg)を参照してください。

修正済みソフトウェア

アップグレードを検討する場合は、http://www.cisco.com/go/psirt と後続のアドバイザリも参照して、問題の解決状況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機器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しいリリースで引き続き適切にサポートされていることの確認を十分に行ってください。情報に不明な点がある場合は、Cisco Technical Assistance Center（TAC）または契約を結んでいるメンテナンス プロバイダーにお問い合せください。

Cisco IOS ソフトウェアの表（下掲）の各行には、Cisco IOS のリリース トレインが記載されています。特定のリリース トレインに脆弱性がある場合は、修正を含む最初のリリース（および、それぞれの予想提供日）が表の「第 1 修正済みリリース」列に記載されます。「推奨リリース」列は、本アドバイザリの公開時点で公開されているすべての脆弱性に対する修正を含むリリースを示します。特定の列に記されているリリースよりも古い（第 1 修正済みリリースより古い）トレインに含まれるリリースが稼働しているデバイスは脆弱であることが確認されています。表の「推奨リリース」列に記載されているリリース、またはそれよりも新しいリリースにアップグレードすることを推奨します。

メジャー リリース	**修正済みリリースの入手可能性**
該当する 12.xベースのリリース	**First Fixed Release（修正された最初のリリース）**
12.0 ~ 12.3	12.0 ~ 12.3ベースのリリースは影響を受けません
Affected 12.4-Based Releases	**First Fixed Release（修正された最初のリリース）**
12.4MD	脆弱性なし
12.4MDA	12.4(24)MDA5より前のすべての12.4MDAリリースが影響を受けます。最初の修正は12.4(24)MDA5
12.4MDB	脆弱性なし
該当する 15.Xベースのリリース	**First Fixed Release（修正された最初のリリース）**
15.0 ~ 15.1	15.0 ~ 15.1ベースのリリースは影響を受けません

不正利用事例と公式発表

Cisco PSIRT では、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は確認し

ておりません。

この脆弱性は内部テストで発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110706-csg

改訂履歴

リビジョン 1.0	2011年7月6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。