コンテント スイッチング モジュールにおけるサービス拒否の脆弱性

High

アドバイザリーID : cisco-sa-20070905-csm
初公開日 : 2007-09-05 16:00
バージョン 1.1 : Final
CVSSスコア : 7.8
回避策 : No Workarounds available
Cisco バグ ID :

CVE-2007-4789
CVE-2007-4788

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 Switching Module（CSM; コンテント スイッチング モジュール）および Cisco Content Switching Module with SSL（CSM-S）には、サービス拒否（DoS）状態につながる可能性がある 2 つの脆弱性が含まれています。1 つ目の脆弱性は TCP パケットを処理する際に存在し、2 つ目の脆弱性はサービス ターミネーションが有効になっているデバイスに該当します。

Cisco では、該当するお客様用に、これらの脆弱性に対応する無償ソフトウェアを提供しております。

このアドバイザリは、https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070905-csm で公開されています。

該当製品

脆弱性のある製品

これらの脆弱性は CSM ソフトウェア バージョン 4.2 および CSM-S ソフトウェア バージョン 2.1 で発見されたものです。これらの製品のうち、脆弱性を含むソフトウェア バージョンを次の表に示します。

脆弱性	CSM	CSM-S
TCP パケット処理による DOS	4.2.3a より古い 4.2	2.1.2a より古い 2.1

サービス ターミネーション	4.2.7 より古い 4.2	2.1.6 より古い 2.1

コンテント スイッチング モジュールで実行されているソフトウェアを確認するには、Catalyst スイッチにログインし、show version コマンドを発行します。

次の例では、CatOS が稼働するスーパーバイザで CSM ソフトウェア バージョン 4.2(2) が実行されています。CatOS または IOS が稼働するスーパーバイザでは、同様の出力が表示されます。次の出力が示すように、CSM のバージョンは WS-X6066-SLB-APC というラベルが付いたモジュールに対して表示されます。

```
<#root>

Console>

show version

WS-C6506 Software, Version NmpSW: 7.6(9)
Copyright (c) 1995-2004 by Cisco Systems
NMP S/W compiled on Aug 27 2004, 20:05:14

System Bootstrap Version: 7.1(1)
System Boot Image File is 'disk0:cat6000-sup2k8.7-6-9.bin'
System Configuration register is 0x2102

Hardware Version: 3.0  Model: WS-C6506  Serial #: TBA05360375

PS1  Module: WS-CAC-1300W    Serial #: ACP05061071
PS2  Module: WS-CAC-1300W    Serial #: ACP05060407

Mod Port Model               Serial #    Versions
--- ---- ------------------- ----------- --------------------------------------
1   2    WS-X6K-SUP2-2GE     SAD055104YY Hw : 3.2
                                         Fw : 7.1(1)
                                         Fw1: 6.1(3)
                                         Sw : 7.6(9)
                                         Sw1: 7.6(9)
         WS-F6K-PFC2         SAD055104H5 Hw : 3.0
                                         Sw :
         WS-X6K-SUP2-2GE     SAD055104YY Hw : 3.2
                                         Sw :
2   48   WS-X6248-RJ-45      SAD0501084U Hw : 1.4
                                         Fw : 5.4(2)
                                         Sw : 7.6(9)

5   4    WS-X6066-SLB-APC    SAD105003DW Hw : 1.9
                                         Fw :
                                         Sw : 4.2(2)


       DRAM                    FLASH                   NVRAM
Module Total   Used    Free    Total   Used    Free    Total Used  Free
------ ------- ------- ------- ------- ------- ------- ----- ----- -----
1      262144K  70354K 191790K  32768K  23251K   9517K  512K  253K  259K

Uptime is 43 days, 22 hours, 7 minutes
```

次の設定セグメントは、サービス ターミネーションが有効になっている vserver を示しています。

```
vserver WWW:2
  virtual x.x.x.x  tcp www service termination
```

脆弱性を含んでいないことが確認された製品

これらの脆弱性に該当するのは、上に示す 4.2 バージョンが稼働している Catalyst CSM モジュールだけです。CSM ソフトウェア バージョン 4.1、3.2、および 3.1 は、これらの脆弱性には該当しません。

上に示す 2.1 バージョンが稼働している Catalyst CSM-S モジュールは、これらの脆弱性に該当します。

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。Cisco Secure Content Accelerator は、これらの脆弱性には該当しません。

詳細

Catalyst CSM は、Catalyst 6500 および 7600 シリーズ用の統合サーバ ロード バランシング ラインカードであり、サーバ、キャッシュ、ファイアウォール、Secure Sockets Layer（SSL）デバイス、VPN ターミネーション デバイスなどのエンド ポイントへのクライアント トラフィックの応答時間を改善します。

Catalyst 6500 CSM-S は、高性能のサーバ ロード バランシング（SLB）と Secure Socket Layer（SSL）オフロードを組み合せた製品です。CSM-S は CSM と似ていますが、CSM-S では SSL で暗号化されたトラフィックを終端または送信することができるので、インテリジェントなロード バランシングを実行しながら、エンドツーエンドの暗号化を実現します。

この脆弱性に該当するコードを実行しているモジュールが特定の TCP パケットを順不同で受信すると DoS 状態が発生し、CPU 使用率が 100 % に達したり、icp.fatPath length エラーを伴う FPGA4 例外によりリロードが発生する可能性があります。

この脆弱性は、Cisco Bug ID CSCsd27478(登録ユーザ専用)に記載されています。

この脆弱性に該当するソフトウェアを実行しているモジュールでサービス ターミネーションが有効になっていて、ネットワーク使用率が高くなると、DoS 状態が発生し、FPGA4 例外の 1 IDLE エラーによりリロードが発生する可能性があります。

この脆弱性は、Cisco Bug ID CSCsh57876(登録ユーザ専用)に記載されています。

通常の場合、CSM および CSM-S の管理は MSFC の CLI によって処理されますが、ソフトウェアをアップグレードするには、スイッチにログインしてからモジュールとのセッションを開始する必要があります。

CSM をアップグレードする方法についての詳細は、Cisco.com の http://www.cisco.com/JP/support/public/ht/tac/100/1007661/csm_upgrade-j.shtml ページを参照してください。

CSM-S をアップグレードする方法については、http://www.cisco.com/en/US/docs/interfaces_modules/services_modules/csms/2.1.1/configuration/guide/g を参照してください。

回避策

これらの脆弱性に対する回避策はありません。サービス ターミネーションを削除すると Cisco Bug ID CSCsh57876 は緩和されますが、この機能を無効にするとデバイスの動作に対して重要な役割を果たすサービスも無効になる可能性があります。

Cisco 機器に適用可能な追加の軽減策については以下の "Cisco Applied Intelligence companion document" より入手可能です。

https://sec.cloudapps.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20070905-csm

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。

「リビルド」および「メンテナンス」という用語の詳細については、次のURLを参照してください。http://www.cisco.com/warp/public/620/1.html

登録ユーザは、http://www.cisco.com/pcgi-bin/tablebuild.pl/cat6000-csm?psrtdcat20e2（登録ユーザ専用）から CSM の修正済みソフトウェアを入手できます。

登録ユーザは、http://www.cisco.com/pcgi-bin/tablebuild.pl/cat6000-csms?psrtdcat20e2（登録ユーザ専用）から CSM-S の修正済みソフトウェアを入手できます。

推奨事項

$propertyAndFields.get("recommendations")

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。

これらの脆弱性は、カスタマー サポート ケースの調査中に発見されたものです。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070905-csm

改訂履歴

リビジョン 1.1	2008年4月25日	CSCsh57876およびCSCsd27478のCVSSスコアへのリンクを更新。
リビジョン 1.0	2007 年 9 月 5 日	初版リリース

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。

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。