Cisco 11500 Content Services SwitchのSSL不正クライアント証明書の脆弱性

severity

アドバイザリーID : cisco-sa-20051019-css

初公開日 : 2005-10-19 16:00

バージョン 1.1 : 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

Secure Socket Layer(SSL)ターミネーションサービスで設定されたCisco CSS 11500シリーズコンテンツサービススイッチ(CSS)は、不正なクライアント証明書を処理する際のサービス拒否(DoS)攻撃に対して脆弱です。シスコでは、この脆弱性に対処する無償ソフトウェアを提供しています。この脆弱性に対しては、影響を緩和するための回避策があります。

このアドバイザリは、https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20051019-css で公開されています。

該当製品

このセクションには、該当製品に関する詳細が掲載されています。

脆弱性のある製品

次のバージョンのCisco WebNSオペレーティングシステムを実行しているCisco CSS 11500シリーズコンテンツサービススイッチ

- 7.1
- 7.2
- 7.3
- 7.4
- 7.5

CSSで実行されているCisco WebNSのバージョンは、次のコマンドを実行することで確認でき

ます。

```
# show version
```

脆弱性を含んでいないことが確認された製品

Cisco CSS 11000 シリーズ コンテンツ サービス スイッチ

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 CSS 11500コンテンツサービススイッチは、データセンターに堅牢でスケーラブルなネットワークサービス（レイヤ4 ～ 7）を提供するように設計されたロードバランシングデバイスです。Cisco CSS 11500は、プロトコルヘッダーの分析を実行し、設定可能なポリシーに基づいて適切なリソースに要求を送信します。統合されたSSLモジュールにより、Cisco CSS 11500はデジタル証明書の管理を簡素化し、SSLアクセラレーションサービスを提供してパフォーマンスを最適化できます。

Cisco CSS 11500は、SSLセッションのネゴシエーション中に不正なデジタルクライアント証明書を提示すると、メモリ不良の問題が原因でリロードする可能性があります。この状況は、CSSがSSLセッションのネゴシエーション中にクライアント証明書を要求しなかった場合でも発生します。この脆弱性は、SSL終端サービスをサポートするようにCSSが設定されている場合にのみ存在します。SSL終端サービスはデフォルトでは設定されていません。

SSL終端サービスがCSSで設定されているかどうかを確認するには、次の手順を実行します。

- 現在の実行コンフィギュレーションを表示します。

```
# show running-config
```

- 設定の[Services]セクションで、有効なSSL終端サービスを検索できます。**ssl-serv1**という名前の有効なSSL終端サービスの例は、次のようになります。**type**コマンドに**ssl-accel**または**ssl-accel-backend**オプションを付けた場合、サービスがSSLモジュールに関連付けられていることを示し、**active**コマンドを使用した場合は、SSL終了サービスが有効になっていることを示します。

```
service ssl-serv1
        type ssl-accel
        slot 3
        keepalive type none
        add ssl-proxy-list ssl list1
        active
```

この脆弱性は、次のCisco Bug IDに記載されています。

- **CSCee64771(登録ユーザ専用):SSLを実行するCSSが不正なクライアント証明書を使用してクラッシュする可能性がある**

回避策

回避策の効果は、製品の組み合わせ、ネットワークトポロジ、トラフィックの動作、組織のミッションなど、お客様の状況によって異なります。該当する製品とリリースは多岐に渡るので、サービス プロバイダーやサポート機関に連絡し、ネットワーク内で使用するのに最も適した回避策を確認してから、実際に配備することを推奨いたします。

Cisco WebNSソフトウェアの修正済みバージョンにアップグレードできない場合は、次の回避策を使用できます。

- 不要な場合は、ネットワークサービスのSSL終端を無効にします。
  サービスコンフィギュレーションモードでは、次のコマンドを使用してSSLサービスを無効にできます。**ssl-serv1**は、ユーザ定義のSSLサービスの名前です。

  ```
  (config)# no service ssl-serv1
  Delete service <ssl>, [y/n]:y
  ```

  Cisco WebNS 7.40を実行するCSSでのSSLサービスの設定に関するドキュメントは、http://www.cisco.com/en/US/products/hw/contnetw/ps792/products_configuration_guide_book09186a008027ab4e.htmlにあります。
  Cisco WebNS 7.50を実行するCSSでのSSLサービスの設定に関するドキュメントは、http://www.cisco.com/en/US/products/hw/contnetw/ps792/products_configuration_guide_book09186a0080405453.htmlにあります。

- CSSまたはCSSの前にあるネットワークデバイスでアクセスコントロールリスト(ACL)を使用して、信頼できるネットワークへのSSL終端サービスへのアクセスを制限します。
  Cisco WebNS 7.40を実行するCSSでのACLの設定に関するドキュメントは、http://www.cisco.com/en/US/products/hw/contnetw/ps792/products_configuration_guide_chapter09186a008029b1db.html#wp1133930にあります。
  Cisco WebNS 7.50を実行するCSSでのACLの設定に関するドキュメントは、http://www.cisco.com/en/US/products/hw/contnetw/ps792/products_configuration_guide_chapter09186a008040aeb9.html#wp1133930にあります。

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/en/US/products/products_security_advisories_listing.html と後続のアドバイザリを参照して、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。情報が明確でない場合は、Cisco Technical Assistance Center(TAC)に連絡して支援を求めてください。

リリース群	修正済みリリース
7.3	7.30.4.02 以降
7.4	7.40.2.02 以降
7.5	7.50.1.03 以降

Cisco WebNS 7.10および7.20をご使用のお客様は、CSSプラットフォームをCisco WebNS 7.30以降の修正済みバージョンにアップグレードすることをお勧めします。修正済みソフトウェアは、登録ユーザがhttp://www.cisco.com/pcgi-bin/tablebuild.pl/css11500-maint?psrtdcat20e2から入手できます。

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。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20051019-css

改訂履歴

リビジョン 1.1	2005年10月19日	「ソフトウェアバージョンと修正」の表に修正済みソフトウェアへの直接リンクを追加。
リビジョン 1.0	2005年10月19日	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。

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。