SSL 実装脆弱性

Medium	**アドバイザリーID :** cisco-sa-20030930-ssl **初公開日 :** 2003-09-30 23:30 **バージョン 2.2 :** Final **CVSSスコア :** 5.0 **回避策 :** Yes **Cisco バグ ID :**	CVE-2003-0544 CVE-2003-0545 CVE-2003-0543 CVE-2003-0851 CVE-2005-1247

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

2003 年 9月 30 日で、SSL のための OpenSSL 実装 の新しい脆弱性は発表されました。 これはようにこの文書の「最初」脆弱性参照されます。

2003 年 11月 4 日で、SSL のための OpenSSL 実装 の別の脆弱性は、バージョン 0.9.6、発表されました。 これはようにこの文書の「二番目に」脆弱性参照されます。

OpenSSL 影響を受けた実装に基づいて SSL サーバを実行する影響を受けたネットワークデバイスはクライアントによって不正 な 認証と示されたときサービス拒絶 （ DoS ） 攻撃に脆弱かもしれません。 ネットワークデバイスはクライアントからの証明書を認証しないことを設定してもこの脆弱性に脆弱かもしれません。 これら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 http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20030930-ssl で掲示されます。

該当製品

修正済みソフトウェア

以下の製品に OpenSSL コードに基づいて SSL 実装があり、OpenSSL 最初の脆弱性から影響を受けるかもしれません。

- 12.1E リリース トレインの Cisco IOS 12.1(11)E およびそれ以降
  注: 暗号画像だけ（56i および k2）Cisco 7100 および 7200 シリーズ ルータのために脆弱です。
- Cisco IOS 12.2SX および 12.2SY リリース トレイン
  注: 暗号画像だけ（k8、k9 および k91）のためにおよび Cisco 7600 シリーズ ルータ 脆弱 Cisco Catalyst 6500 シリーズです。
- Cisco PIX ファイアウォール
- Cisco Catalyst 6500 シリーズおよび Cisco 7600 シリーズ ルータのための Cisco Firewall サービス モジュール（FWSM）
- Cisco Catalyst 6000 および 6500 シリーズ スイッチおよび Cisco 7600 シリーズ ルータのための Ciscoネットワーク 分析 モジュール（NAM）
- Ciscoコンテンツサービススイッチ（CSS）11000 シリーズ
- Ciscoコンテンツサービススイッチ（CSS）セキュアコンテンツアクセラレータ バージョン 1 及び 2
- Cisco Threat Response（CTR）
- Cisco グローバルサイトセレクタ（GSS）4480
- Ciscoアプリケーション及び Content Networking Software（ACNS）
- Cisco SN 5428 ストレージ ルータ
- CiscoWorks 1105 Hosting Solution Engine（HSE）
- CiscoWorks 1105 Wireless LAN Solution Engine（WLSE）
- CiscoWorks Common Services（CMF）
- Cisco SIP Proxy Server（SPS）
- Cisco Secure Policy Manager（CSPM）

以下の製品に OpenSSL コードに基づいて SSL 実装があり、OpenSSL 第 1 及び第 2 脆弱性から影響を受けるかもしれません。

- Cisco PIX ファイアウォール
- Cisco Catalyst 6500 シリーズおよび Cisco 7600 シリーズ ルータのための Cisco Firewall サービス モジュール（FWSM）
- Ciscoコンテンツサービススイッチ（CSS）11000 シリーズ- SCM だけ影響を受けています
- Cisco SN 5428 ストレージ ルータ

脆弱性を含んでいないことが確認された製品

SSL が実装されている以下の製品は OpenSSL 脆弱性に*脆弱*であるために現在知られています。

- Cisco VPN 3000 シリーズ コンセントレータ
- Cisco Secure Intrusion Detection System（NetRanger）アプライアンス。 これには IDS-42xx アプライアンスが、NM-CIDS および WS-SVS-IDSM2 含まれています。
- Cisco Catalyst 6500 シリーズおよび Cisco 7600 シリーズ ルータのための Cisco Secure ソケット 層（SSL）サービス モジュール
- Cisco Call Manager

CatOS は SSL が実装されないし、脆弱ではないです。 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。

改訂履歴

Revision 2.2	2004-21-Jan	複数の製品のための更新済修正済みリリース 情報およびアベイラビリティ。
Revision 2.1	2003-07-Nov	OpenSSL 第 2 脆弱性から影響を受けるために知られている明白にされた製品。 影響を受けた製品として追加された Cisco CSS 11000 シリーズ（SCM だけ）。 CSPM のための追加されたソフトウェアが利用可能な日付。
Revision 2.0	2003-04-Nov	OpenSSL 第 2 脆弱性に追加された情報。
リビジョン 1.3	2003-13-Oct	影響を受ける追加された CSPM。 更新済 SCA および NAM 修正済みソフトウェア ステータス。
リビジョン 1.2	2003-02-Oct	「該当製品では」および影響を受けていますとして" Details "セクション、追加された CSA および CTR。 「ソフトウェア バージョン および 修正」セクションでは、影響を受けた IOSイメージについての更新された情報。
リビジョン 1.1	2003-30-Sept	影響を受けた IOSイメージについての更新された情報。
リビジョン 1.0	2003-30-Sept	初回公開リリース

利用規約

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。