Transport Layer Security 再ネゴシエーション脆弱性

severity	**アドバイザリーID :** cisco-sa-20091109-tls	CVE-2009-3555
	初公開日 : 2009-11-09 13:00	
	最終更新日 : 2011-10-20 15:47	
	バージョン 1.15 : Final	
	回避策 : Yes	
	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

TLS および SSL のバージョンを使用する Cisco製品に影響を与える可能性がある Transport Layer Security （ TLS ）プロトコルで存在 する業界全体脆弱性。 存在 する脆弱性プロトコルがどのようにでセッション 再ネゴシエーションを処理し、潜在的な man-in-the-middle攻撃--にユーザをさらすか。

このアドバイザリは http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20091109-tls で掲示されます。

該当製品

修正済みソフトウェア

このセクションは時更新済です。 以下の製品は脆弱であるために確認されます:

- Cisco インターネット吹流し CD
- Cisco ACE 4700 シリーズ Application Control Engine Appliance
- Cisco ACE アプリケーション コントロール エンジン モジュール
- Cisco ACE GSS 4400 シリーズ グローバル サイト セレクタ アプライアンス
- Cisco ACE Web Application Firewall
- Cisco Wireless Control System
- Cisco Wireless LAN Controller （ WLC ）

  注: Â Extensible Authentication Protocol （ EAP ） Transport Layer Security （ EAP-TLS ）および Protected Extensible Authentication Protocol （ PEAP ）はこの脆弱性から影響を受け

ません。

-
- Cisco Wireless Location Appliance
- CiscoWorks Wireless LAN Solution Engine（WLSE）
- Cisco デジタル Media Player
- Cisco Digital Media Manager
- Cisco Access Control Server（ACS）
- CiscoWorks Common Services
- Cisco TelePresence Recording Server
- Cisco NX-OS ソフトウェア
- Cisco Video Surveillance オペレーション マネージャ ソフトウェア
- Cisco Video Surveillance メディア サーバ ソフトウェア
- Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス
- Catalyst 6500 シリーズおよび Cisco 7600 シリーズ Firewall Services Module（FWSM）
- Cisco AVS 3120 および 3180 シリーズ Application Velocity System（AVS）
- Cisco CSS 11500 シリーズ コンテンツ サービス スイッチ
  CSS 11500 シリーズ コンテンツ サービス スイッチはデフォルト 設定を用いるこの脆弱性から影響を受けます。 ただし、クライアント認証 機能は軽減/ソリューションとして有効に することができます。
  バーチャル SSL サーバのクライアント認証をディセーブルにするために有効に するか、または、**ssl-proxy-list** の下で ssl **サーバ <number> 認証コマンドを**使用して下さい。
  注: デフォルトで **Â は**、クライアント認証無効です。 CSS のクライアント認証を有効にした後、クライアント 認証を確認するのに CSS が使用する CA 認証を規定 して下さい。
-
- Cisco コンテンツ スイッチング モジュール（CSM）
- Cisco Wide Area Application Services（WAAS）
- Cisco Application Networking Manager（ANM）
- Cisco Unified IP Phone
- Cisco ONS 15500 シリーズ
- Cisco Unified Contact Center 製品
- Cisco Security Agent（CSA）
- Cisco IP Communicator
- Cisco Network Registrar
- Cisco Unified Communications Manager（CallManager）
- Cisco Network Analysis Module（NAM）ブレード ソフトウェア（NAM）
- Cisco IronPort E メール セキュリティ アプライアンス（X シリーズ及び Cシリーズ）
- Cisco スパム及びウイルス ブロッカー（B シリーズ）
- Cisco IronPort Web セキュリティ アプライアンス（S シリーズ）
- Cisco IronPort セキュリティ管理 アプライアンス（M シリーズ）
- Cisco IronPort 暗号化 アプライアンス（国際エネルギー機関）
- Cisco Catalyst 6500 シリーズ SSL サービス モジュール
- Cisco PIX

http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/prod_eol_notices_list.html。

脆弱性を含んでいないことが確認された製品

以下の製品は確認された脆弱です:

- Cisco AnyConnect VPN Client
- Cisco Unified MeetingPlace
- Cisco Data Center Network Manager
- Cisco Service Control Subscriber Manager
- Cisco Secure Desktop（CSD）
- Cisco ASA Advanced Inspection and Prevention（AIP）セキュリティ サービス モジュール
- Cisco Transport Manager（CTM）
- Cisco IOS SSL VPN
- Cisco IOS HTTP セキュアサーバ
- Cisco 侵入防御システム（CIDS/IPS）

このセクションは時更新済です。

改訂履歴

Revision 1.15	2011-October-20	更新済脆弱性が存在する製品および脆弱性が存在しない製品
Revision 1.14	2010-July-22	更新済脆弱性が存在する製品
Revision 1.13	2010-March-29	CUCM のための更新済修正済みソフトウェアバージョン
Revision 1.12	2010-March-10	WAAS および WLC のための更新済修正済みソフトウェアバージョン
Revision 1.11	2010-March-03	セキュア IOS HTTP は脆弱性が存在しない製品に追加されて保護します
Revision 1.10	2010-February-26	更新済修正済みソフトウェア
Revision 1.9	2010-February-05	更新済該当製品および詳細セクション
Revision 1.8	2010-January-21	更新済ソフトウェア修正プログラム表および脆弱性が存在しない製品
Revision 1.7	2010-January-04	該当製品 アップデート。

Revision 1.6	2009-December-18	該当製品および詳細更新。
Revision 1.5	2009-December-14	脆弱 で はない EAP-TLS および PEAP。
リビジョン 1.4	2009-December-4	詳細および影響アップデート。
リビジョン 1.3	2009-December-3	該当製品 アップデート。
リビジョン 1.2	2009-November-18	該当製品 アップデート。
リビジョン 1.1	2009-November-16	該当製品 アップデート。
リビジョン 1.0	2009-November-9	初回公開リリース

Â

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。