

Cisco OpenSSL 実装脆弱性

severity	アドバイザーID : cisco-sa-20040317-openssl	CVE-2004-0079
	初公開日 : 2004-03-17 13:00	CVE-2004-0112
	バージョン 1.6 : Final	CVE-2004-0081
	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

SSL のための [OpenSSL](#) 実装の新しい脆弱性は 2004 年 3月 17 日発表されました。

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サービス拒絶 (DoS) 攻撃に脆弱かもしれません。利用可能な回避策がこのアドバイザーの Workaround セクションのこの脆弱性 on Cisco 軽減するために製品の効果をあります。Cisco は利用可能なとき修正済みソフトウェアを提供して、それにことを顧客 アップグレード推奨します。

このアドバイザーは <http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20040317-openssl> 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、この脆弱性から影響を受けます。

- Cisco 7100 および 7200 シリーズ ルータのための 12.1E リリーストレインの Cisco IOS 12.1(11)E およびそれ以降。暗号画像だけ (56i および k2) 脆弱です。
- Cisco IOS 用のおよび Cisco 7600 シリーズ ルータ 12.2SY および 12.2ZA リリーストレイン Cisco Catalyst 6500 シリーズ。暗号画像だけ (k8、k9 および k91) 脆弱です。
- 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 MDS 9000 シリーズ マルチレイヤ スイッチ
- Cisco コンテンツサービス スイッチ (CSS) 11000 および 11500 シリーズ
- Cisco グローバル サイトセレクタ (GSS) 4480 および 4490
- 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 (SCA) バージョン 1 及び 2
- CiscoWorks Common Services (CWCS) バージョン 2.2 および CiscoWorks Common Management Foundation (CMF) バージョン 2.1
- Cisco Access Registrar (CAR)
- Cisco Call Manager (CCM)
- Cisco Okena Stormwatch 3.2
- Cisco アプリケーション 及び Content Networking Software (ACNS)
- [Cisco Threat Response \(CTR \)](#)

以下の製品に OpenSSL コードに基づいて SSL 実装があり、この脆弱性から影響を受けません。

- 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 SN 5428 および SN 5428-2 ストレージ ルータ
- Cisco CNS Configuration Engine
- 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 SIP Proxy Server (SPS)
- CiscoWorks 1105 Hosting Solution Engine (HSE)
- CiscoWorks 1105 Wireless LAN Solution Engine (WLSE)
- Cisco Ethernet Subscriber Solution Engine (ESSE)

SSL が実装されている以下の製品はこの脆弱性から影響を受けません。

- Cisco VPN 3000 シリーズ コンセントレータ
- 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

脆弱性を含んでいないことが確認された製品

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。この脆弱性はまだシスコ製品を渡ってアクティブに調査されて、いくつかの製品のステータスはまだ判別されてしまいました。

改訂履歴

Revi	2004-	更新済 CTR および MDS 9000 修正済み
------	-------	---------------------------

sion 1.6	April-8	リリース 情報。
Revi sion 1.5	2004- April-1	CWCS のための追加された詳細。更新 済 CSS 修正済みリリース 情報。
リビ ジヨ ン 1.4	2004 年 3 月 26 日	CCM のための追加された詳細および GSS、CSS および SCA。
リビ ジヨ ン 1.3	2004- March- 23	FWSM のための有効 日付を変更して下 さい。ACNS のための追加された詳細。
リビ ジヨ ン 1.2	2004- March- 19	影響を受けた製品リストに IOS 12.2ZA リリーストレイン、CSS SCA、ACNS、 CTR、GSS 4490 および CSS 11500 シ リーズを追加しました。PIX により多く の詳細を追加しました。
リビ ジヨ ン 1.1	2004- March- 18	追加された CCM、影響を受ける Okena Stormwatch。影響を受けない 6500/7600 のための追加された SSL モジ ュール。影響を受けたセクションの IOS リリースで詳しく説明される。
リビ ジヨ ン 1.0	2004- March- 17	初期リリース。

利用規約

本アドバイザー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。本アドバイザー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。

本アドバイザーの記述内容に関して情報配信の URL を省略し、単独の転載や意識を施した場合、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。