OpenSSL バージョン ロールバックおよび AlgorithmÂ 弱い暗号脆弱性

Medium	**アドバイザリーID :** Cisco-SA-20051012-CVE-2005-2969 **初公開日 :** 2005-10-12 15:54 **最終更新日 :** 2015-01-31 09:00 **バージョン 29.0 :** Final **CVSSスコア :** 4.3 **回避策 :** No Workarounds available **Cisco バグ ID :**	CVE-2005-2969 CVE-2005-2946

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

OpenSSL は非認証を可能にする可能性があるセキュリティ制限をバイパスするために脆弱性がリモート攻撃者含まれています。

最初の脆弱性（CVE-2005-2969）は OpenSSL バージョン 0.9.7g によっておよび前に提供される SL/TLS サーバ実装を使用してアプリケーションに影響を与えます。 これらの実装にイネーブルになっているサード パーティ バグを軽減するように設計されているオプションがある場合 man-in-the-middle攻撃を行なうリモート攻撃者は SSL プロトコルの 2.0 バージョンを使用するためにホスト間の接続を強制する可能性があります。 SSL 2.0 プロトコルで存在 する 既知暗号弱さ。

0.9.8a 前に OpenSSL バージョンのデフォルト 設定で存在 する 2つめの脆弱性（CVE-2005-2946）。 この設定は MD5 を使用してメッセージ要約を作成します。 暗号化アルゴリズムの弱さはリモート攻撃者が有効な認証局シグニチャが付いている証明書を造ることを可能にする可能性があります。

OpenSSL は Security Advisory のこの脆弱性を確認し、更新をリリースしました。

攻撃者は man-in-the-middle攻撃 ベクトルによるこれらの脆弱性を不正利用してまずないです。 そのような不正侵入はリアルタイムに 2 つのホスト間のトラフィックを代行受信し、修正することの要件が原因で行って非常に困難です。 Man-in-the-middle攻撃は顧客とサービス プロバイダー間のデバイスか接続に物理アクセスを用いる攻撃者によってだけ使用可能一般的にです。

MD5 アルゴリズムの弱さのいくつかのデモが最近ずっとあります。 MD5 は技術的に壊れている間、不確かではないです。 攻撃者が正常に擬似証明書のことを署名の使用のための MD5 衝突を作成する可能性があることはまずないです。

管理者はこれらの問題のの特別な関心を奪取 するべきではありません。 管理者は更新バージョンの完全なテストが完了するまで生産システムをアップデートするために待っていることを考慮するかもしれません。 これらの問題の心配が起こる場合、管理者は IE 3.x Compatibility フラグを取除くことを考えるかもしれません。

該当製品

OpenSSL は次のリンクで Security Advisory をリリースしました: secadv_20051011

Apple は次のリンクでセキュリティ 発表をリリースしました: セキュリティ更新プログラム 2005-009
Astaro は次のリンクでセキュリティ 発表をリリースしました: Up2Date 4.029、Up2Date 5.208 および Up2Date 6.101

Avaya は次のリンクで Security Advisory をリリースしました: ASA-2006-031 および ASA-2006-260

Blue Coat は次のリンクで Security Advisory をリリースしました: Blue Coat Security Advisory

Cisco は次のリンクで Cisco バグ ID CSCsc27533、CSCej54402、CSCsc48330、CSCsc33835、CSCsc58356 および CSCek01123 をアドレス指定するためにセキュリティ応答をリリースしました: 68324

Debian は次のリンクで Security Advisory をリリースしました: DSA-875-1、DSA-881-1、DSA-882-1 および DSA-888-1

FreeBSD は FTP 次のリンクで Security Advisory をリリースしました: FreeBSD-SA-05:21.openssl

Gentoo は次のリンクで Security Advisory をリリースしました: GLSA 200510-11

HP は FTP 次のリンクで PDF 形式の該当製品のリストを発表しました: HP. HP は次のリンクで Security Advisory をリリースしました: HPSBUX02174 および HPSBUX02186

日立社は次のリンクで Security Advisory をリリースしました: HS06-022-01 および HS07-016

IBM は次のリンクで脆弱性説明をリリースしました:

SSRVHMCHMC_C081516_474
SSRVHMCHMC_C081516_604
SSRVHMCHMC_C081516_754

Juniper は次のリンクでセキュリティ情報を発表しました: PSN-2005-12-025

Mandriva は次のリンクで Security Advisory をリリースしました: MDKSA-2005:179

NetBSD は FTP 次のリンクで Security Advisory をリリースしました: NetBSD-SA2005-010

OpenPKG は次のリンクで Security Advisory をリリースしました: OpenPKG-SA-2005.022

Red Hat は次のリンクで Security Advisory をリリースしました: RHSA-2005:800、RHSA-2005:882、RHSA-2008:0264、RHSA-2008:0525 および RHSA-2008:0629

SCO グループは FTP 次のリンクで Security Advisory をリリースしました: SCOSA-2005.48

SGI は FTP 次のリンクで Security Advisory をリリースしました: 20051003-01-U

Slackware は次のリンクで Security Advisory をリリースしました: SSA:2005-286-01

SUN は次のリンクでアラート 通知を再リリースしました: 201126

SUSE は次のリンクでセキュリティ 発表をリリースしました: SUSE-SA:2005:061

Trustix は次のリンクで Security Advisory をリリースしました: TSLSA-2005-0057 および TSLSA-2005-0059

Ubuntu Linux は次のリンクでセキュリティ通知を公開しました: USN-179-1 および USN-204-1

脆弱性のある製品

OpenSSL バージョン 0.9.7h を稼動するシステムはまたは前に脆弱です。

脆弱性を含んでいないことが確認された製品

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。

回避策

管理者は適切なアップデートを適用するように助言されます。

管理者は OpenSSL アプリケーションの SSL プロトコルの 2.0 バージョンを無効に するように助言されます。

管理者は検討してください影響を受けたフラグ SSL ロールバック脆弱性を軽減するかもしれません。

修正済みソフトウェア

OpenSSL は次のリンクでパッチをリリースしました: patch-CAN-2005-2969.txt

更新バージョンは次のリンクで利用できます: OpenSSL 0.9.7h か 0.9.8a

Apple は次のリンクで更新をリリースしました:

Mac OS X 10.3.9 クライアント
Mac OS X 10.3.9 サーバ
Mac OS X 10.4.3 クライアント
Mac OS X 10.4.3 サーバ

Astaro は FTP 次のリンクで Astaro セキュリティ Linux のための更新済パッケージをリリースしました: Astaro 5.208 および Astaro 6.101。 ユーザはまた **up2date** コマンドの発行によって最新のパッケージを得ることができます。

Blue Coat は次のリンクで登録ユーザ向けの更新をリリースしました: Blue Coat

アクティブな契約を持つ Cisco カスタマは次のリンクで Software Center を通して更新を入手できます: Cisco。 契約のない Cisco カスタマは 1-800-553-2447 か 1-408-526-7209 でまたは *tac@cisco.com* で E メールで Cisco Technical Assistance Center にコンタクトをとってアップグレードを入手できます。

Debian は次のリンクで更新済パッケージをリリースしました: Debian 3.0 （ openssl094 ）、Debian 3.0 （ openssl095 ）、Debian 3.1 （ openssl096 ）および Debian 3.0/3.1 （ openssl096c ）

FreeBSD は FTP 次のリンクでパッチをリリースしました: openssl.patch

Gentoo 更新は**出現**コマンドを使用して次のパッケージのために入手することができます: 開発 libs/openssl

HP は次のリンクで更新済 HTTPサーバ バージョンをリリースしました: HP HTTPサーバ 5.97。
HP は次のリンクで HP-UX のための更新済パッケージをリリースしました:

HP-UX 11.11
修正 A.00.09.07I またはそれ以降

HP-UX 11.23
修正 A.00.09.07I.001 またはそれ以降

日立社は更新に利用可能な直通正常な日立社サポート チャネルをしました。

IBM は次の更新をリリースしました:

Juniper は次のリンクで登録ユーザ向けの IVE OS の更新バージョンをリリースしました: IVE OSソフトウェア

Mandriva は **MandrivaUpdate** を使用して自動的にアップデートすることができます。

NetBSD は FTP 次のリンクで更新済パッケージをリリースしました: NetBSD

OpenPKG は FTP 次のリンクで更新済パッケージをリリースしました:

OpenPKG 2.3 - openssl-0.9.7e-2.3.3
OpenPKG 2.4 - openssl-0.9.7g-2.4.2

Red Hat パッケージはまたは **yum** コマンド **up2date** を使用して更新済である場合もあります。

SCO グループは FTP 次のリンクで更新済パッケージをリリースしました: openssl-0.9.7i.image

SGI は次のリンクで登録ユーザ向けの ProPack 3 サービスパック 6 のためのパッチをリリースしました: パッチ 10235

Slackware パッケージは **upgradepkg** コマンドを使用して更新済である場合もあります。

SUN は次のリンクでパッチをリリースしました:

SPARC
Solaris 10 - 120011-14

Intel
Solaris 10 - 127128-11

SUSE は更新済パッケージをリリースしました; ユーザは **YaST** を使用して更新をインストールできます。

Trustix 製品は **swup** を使用して更新済である場合もあります **----upgrade コマンド**。

Ubuntu は更新済パッケージをリリースしました; ユーザは**アップデート マネージャ**を使用して更新をインストールできます。

不正利用事例と公式発表

Cisco Product Security Incident Response Team（PSIRT）では、本アドバイザリに記載されている脆弱性のエクスプロイト事例やその公表を確認していません。

出典

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/Cisco-SA-20051012-CVE-2005-2969

改訂履歴

Version	Description	Section	Status	日付
1.0	初版リリース	該当なし	Final	2005-Oct-12

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。