OpenSSL RSA シグニチャ偽作脆弱性

Medium	**アドバイザリーID :** Cisco-SA-20060905-CVE-2007-5810 **初公開日 :** 2006-09-05 17:39 **最終更新日 :** 2015-01-31 08:15 **バージョン 61.0 :** Final **CVSSスコア :** 6.4 **回避策 :** No Workarounds available **Cisco バグ ID :**	CVE-2007-5810 CVE-2006-4339

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 バージョン 0.9.7j および前におよび 0.9.8b はおよび前に非認証を可能にする可能性がある正常に造られた X.509 証明書を渡すために脆弱性がリモート攻撃者含まれています。

脆弱性は特定タイプの RSA キーによって署名されたときリモート攻撃者非認証が造られた Public Key Cryptography Standards （ PKCS)#1 バージョン 1.5 シグニチャを渡すようにする可能性があります。 攻撃者は証明書保護されたリソースにアクセスするのに脆弱性を不正利用する可能性があります。

OpenSSL は Security Advisory の脆弱性を確認し、更新バージョンをリリースしました。

この脆弱性は秘密鍵なしでシグニチャを造るのに攻撃者が多分この脆弱性を不正利用する証明書 Authorities.Â によって広く利用されている公開キーの説明者が 3 である場合 PKCS #1 v1.5 シグニチャに影響を与えます。Â PKCS #1 v1.5 は頻繁に X.509 証明書の内で利用されます; 従って、X.509 は証明書脆弱かもしれないことを確認するのに OpenSSL を使用する SSL か TLS のために OpenSSL を使用するソフトウェアを含むすべてのアプリケーション。

該当製品

OpenSSL は次のリンクで Security Advisory をリリースしました: 2006 年 9 月 5 日

Apple は次のリンクでセキュリティ更新プログラムをリリースしました: セキュリティ更新プログラム 2006-007 および Mac OS X 10.4 のための Java リリース 6

ARKOON は次の PDF リンクで Security Advisory をリリースしました: AK-2006-04

Attachmate は次のリンクでテクニカルノートを発表しました: テクニカルノート 2137

Avaya は次のリンクで Security Advisory をリリースしました: ASA-2006-188

Cisco は次のリンクでセキュリティ応答を再リリースしました: Cisco-sr-20061108-openssl. この応答は次のバグID をアドレス指定します:

CSCsg22734
CSCsg01963
CSCsg09619
CSCsg16571
CSCsg17943
CSCsg24311
CSCsg46092
CSCsg04397
CSCsg04386
CSCsg51110
CSCsg51304
CSCek57074
CSCsg59589
CSCsf97055
CSCsg55732
CSCsg36592
CSCsg55738
CSCsg55742
CSCsg56292
CSCsg58599
CSCsg58607
CSCsg58592
CSCsh14665

Debian は次のリンクで Security Advisory をリリースしました: DSA-1173-1 および DSA-1174-1

FreeBSD は FTP 次のリンクで Security Advisory をリリースしました: FreeBSD-SA-06:19

FreeBSD は次のリンクで VuXML 文書を発表しました: openoffice.org ---- 多重 脆弱点

Gentoo は次のリンクで Security Advisory をリリースしました: GLSA 200609-05 および GLSA 200610-06

日立社は次のリンクで Security Advisory をリリースしました: HS07-034

HP は次のリンクでセキュリティ情報を発表しました: HPSBUX02165、HPSBUX02186、HPSBTU02207 および HPSBMA02250

Ingate システムは次のリンクでソフトウェア リリース表記を公開しました: Ingate ファイアウォールおよび Ingate SIParator 4.5.1

Mandriva は次のリンクで Security Advisory をリリースしました: MDKSA-2006:161、MDKSA-2006:177、MDKSA-2006:178 および MDKSA-2006:207

NetBSD は FTP 次のリンクで Security Advisory をリリースしました: NetBSD-SA2006-023

Novell は次のリンクでセキュリティ 発表をリリースしました: Novell 3143224

OpenBSD は次のリンクでセキュリティ 発表をリリースしました: 016: セキュリティ修正: 2006 年 9月 8 日および 011: セキュリティ修正: 2006 年 9月 8 日

OpenOffice.org は次のリンクで Security Advisory をリリースしました: CVE-2006-4339

OpenPKG は次のリンクで Security Advisory をリリースしました: OpenPKG-SA-2006.018

OpenVPN は次のリンクで Security Advisory をリリースしました: OpenVPN 2.0.x 変更ログ

オペラは次のリンクで Security Advisory をリリースしました: 845

Oracle は次のリンクで Security Advisory をリリースしました: BEA07-169.00 および Oracle 重要なパッチアップデート January 2007 年

Red Hat は次のリンクで Security Advisory をリリースしました: RHSA-2006:0661、RHSA-2007:0062、RHSA-2007:0072、RHSA-2007:0073、RHSA-2008:0264、RHSA-2008:0525 および RHSA-2008:0629

SGI は FTP 次のリンクで Security Advisory をリリースしました: 20060901-01-P

Slackware は次のリンクで Security Advisory をリリースしました: SSA:2006-257-02 および SSA:2006-310-01

SSH 通信は次のリンクでソフトウェア リリース メモを発表しました: SSH Tectia サーバ 5.1.1、SSH Tectia マネージャ 2.2.1、IBM z/OS 5.2.1、および SSH Tectia クライアント 5.1.1 の SSH Tectia サーバ

SUN は次のリンクでアラート 通知を再リリースしました: 200196、200474、および 200610

SUN は次のリンクでセキュリティ notifcation をリリースしました: CVE-2006-4339

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:2006:055、SUSE-SA:2006:061 および SUSE-SA:2007:010

SUSE は次のリンクでセキュリティ 要約レポートを発表しました: SUSE-SR:2006:026

Sybase は次のリンクで Security Advisory をリリースしました: 1047991

Trustix は次のリンクで Security Advisory をリリースしました: TSLSA-2006-0051 および TSLSA-2006-0063

Turbolinux は次のリンクで Security Advisory をリリースしました: TLSA-2006-29

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-339-1

ヴァン Dyke Technologies は次のリンクで changelogs を送達しました: SecureCRT 5.2.2 および SecureFX 4.0.2

VMware は次のリンクでナレッジベース記事を発表しました: 3069097 および 9986131。
VMware は次のリンクで Security Advisory をリリースしました: VMSA-2008-0005

US-CERT は次のリンクで脆弱性に関する注記を発表しました: VU#845620

脆弱性のある製品

OpenSSL バージョン 0.9.7jÂ および priorÂ および 0.9.8b はおよび前に脆弱です。

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

管理者は適切な更新を加えるように助言されます。

管理者は 2ファクタ認証認証システムの一部として証明書を利用するように助言されます。

管理者は VPN または影響を受けていない他のリモートアクセス技術の使用によって信頼されたユーザに証明書保護されたリソースへのアクセスを制限することを考えるかもしれません。

DNSSEC を使用して ISC BIND を実行している管理者は利用可能なソフトウェア アップデートを加えるように、すべての古いキーのための新しい RSA-SHA1 および RSA-MD5 キーを生成し、新しいキーにキーロール オーバーを行うように助言されます。

修正済みソフトウェア

OpenSSL は次のリンクで更新バージョンをリリースしました: OpenSSL 0.9.7k および OpenSSL 0.9.8c

Apple は次のリンクで更新済ソフトウェアをリリースしました:

Mac OS X 10.3.9
Mac OS X サーバ 10.3.9
Mac OS X 10.4.8 Intel
Mac OS X 10.4.8 PPC
Mac OS X サーバ 10.4.8 ユニバーサル
Mac OS X サーバ 10.4.8 PPC
Mac OS X 10.4 のための Java

ARKOON は次のリンクで ARKOON 顧客領域のソフトウェア アップデートをリリースしました: クライアントアップデート

Attachmate は次のリンクで更新済パッチをリリースしました: Attachmate

Blue Coat は次のリンクで更新を受信するための手順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 （ openssl ）および Debian （ openssl096 ）

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

FreeBSD は次のリンクでポート収集更新をリリースします: ポート コレクションインデックス

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
app-emulation/emul-linux-x86-baselibs
開発ライブラリ/nss

HP 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:

HP は次のリンクで HP-UX IPv4 のための更新済パッケージをリリースしました:

HP-UX B.11.00
修正 A.2.0.58.01 またはそれ以降

HP-UX B.11.11
修正 A.2.0.58.01 またはそれ以降

HP は次のリンクで HP-UX IPv6 のための更新済パッケージをリリースしました:

HP-UX B.11.11
修正 B.2.0.58.01 またはそれ以降

HP-UX B.11.23
修正 B.2.0.58.01 またはそれ以降

HP は次のリンクで以前のリリース パッチ キットをリリースしました:

- HP Tru64 UNIX v 5.1B-4 - T64KIT1001167-V51BB27-ES-20070321
- HP Tru64 UNIX v 5.1B-3 - T64KIT1001163-V51BB26-ES-20070315
- HP Tru64 UNIX v 5.1A PK6 - T64KIT1001160-V51AB24-ES-20070314
- HP Tru64 UNIX v 4.0G PK4 - T64KIT1001166-V40GB22-ES-20070316
- HP Tru64 UNIX v 4.0F PK8 - DUXKIT1001165-V40FB22-ES-20070316
- （ix）v インターネット Express 6.6 BIND - CPQIM360.SSL.01.tar.gz
- HP 把握管理エージェント-適切な ERP キットにある BIND 9.8.2 パッチをインストールして下さい

HP は次のリンクで更新済ソフトウェアをリリースしました:

- Linux（x86）のための HP システム管理ホームページ 2.1.8-177
- Linux（AMD64/EM64T）のための HP システム管理ホームページ 2.1.8-177
- Windows 2.1.8-179 のための HP システム管理ホームページ

Ingate システムは次のリンクでソフトウェア アップデートをリリースしました: Ingate ファイアウォールおよび Ingate SIParator 4.5.1

インターネット システム コンソーシアムは次のリンクで BIND のための更新済ソフトウェアをリリースしました: BIND 9.2.6-P2 および BIND 9.3.2-P2

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。 Mandrake は **MandrakeUpdate** 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得るための手順をリリースしました: NetBSD

Novell は次のリンクで更新済ソフトウェアをリリースしました: Novell 国際的な暗号インフラストラクチャ（NICI）2.7.2

OpenBSD は FTP 次のリンクでソースコード パッチをリリースしました: OpenBSD 3.8 および OpenBSD 3.9

OpenOffice.org は次のリンクで更新済ソフトウェアをリリースしました: OpenOffice 3.2

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 2.5 - openssl-0.9.8c-2.20060906

OpenVPN は次のリンクで更新済ソフトウェアをリリースしました: OpenVPN 2.0.8

オペラは次のリンクで更新バージョンをリリースしました: オペラ 9.02 またはそれ以降

Oracle は次のリンクで登録ユーザ向けのパッチをリリースしました: Oracle

Oracle は次のリンクで更新済ソフトウェアをリリースしました:

Weblogic server 9.2

- メンテナンス パック 1 へのアップグレード

Weblogic server 9.1

- **スマートなアップデートツール**を使用してパッチ CR295567 をインストールして下さい

Weblogic server 9.0

- バグID CR239280 と関連付けられる 9.0 GA コンボ パッチをインストールして下さい
- パッチ CR295567_900 を加えて下さい

Weblogic server および WebLogic Express バージョン 8.1

- SP6 へのアップグレード
- パッチ CR295567_81sp6 を加えて下さい
- weblogic.jar ファイルの前にクラスパスにパッチのための瓶を置いて下さい

Weblogic server および WebLogic Express バージョン 7.0

- SP7 へのアップグレード
- パッチ CR295567_70sp7 を加えて下さい
- weblogic.jar ファイルの前にクラスパスにパッチのための瓶を置いて下さい

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。

セキュア コンピューティングは更新バージョンをリリースしました。 管理者はアップデートの入手の情報に関してはベンダーに連絡するように勧められます。

SGI は次のリンクで登録ユーザ向けのパッチをリリースしました: パッチ 10332

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。

SSH 通信は次のリンクで更新済ソフトウェアをリリースしました: SSH Tectia ダウンロード

SUN は次のリンクでパッチをリリースしました:

- JDK および JRE 5.0 は 9 およびそれ以降をアップデートします（Windows、Solaris および Linux のために）
- J2SE 5.0

- J2SE 1.0.3_04
- J2SE 1.4.2

SPARC

Intel

J2SE 5.0

Linux プラットフォーム

HP-UX プラットフォーム

AIX プラットフォーム

SUN は次のリンクで関連したプラットフォームの StarOffice/StarSuite のためのパッチをリリースしました: CVE-2006-4339

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。**

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

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。

ヴァン Dyke Technologies は次のリンクで更新済ソフトウェアをリリースしました:

SecureCRT 5.2.2
SecureFX 4.0.2

VMware は次のリンクでパッチをリリースしました:

VMware ESX サーバ 3.0.1
VMware ESX サーバ 3.0.0
VMware ESX サーバ 2.5.4
VMware ESX サーバ 2.5.3
VMware ESX サーバ 2.1.3
VMware ESX サーバ 2.0.2

VMware は次のリンクで更新バージョンをリリースしました:

VMware ACE 1.0.5
VMware ACE 2.0.1 またはそれ以降

VMware プレイヤー 1.0.6
VMware プレイヤー 2.0.3
VMware ワークステーション 5.5.6
VMware ワークステーション 6.0.3
VMware サーバ 1.0.5

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-20060905-CVE-2007-5810

改訂履歴

Version	Description	Section	Status	日付
1.0	初版リリース	該当なし	Final	2006-Sep-05

利用規約