Transport Layer Security(TLS)再ネゴシエーションにおけるリモートの中間者攻撃の脆弱性

Medium

アドバイザリーID : Cisco-SA-20091105-CVE-2009-3555
初公開日 : 2009-11-05 19:53
最終更新日 : 2012-08-14 16:24
バージョン 75.0 : Final
CVSSスコア : 4.3
回避策 : No Workarounds available
Cisco バグ ID :

CVE-2009-3555

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

Multiple Transport Layer Security(TLS)の実装には、TLSセッションを再ネゴシエートする際に、認証されていないリモートの攻撃者が中間者攻撃を実行できる可能性のある脆弱性が存在します。

この脆弱性は、TLS再ネゴシエーションプロセス中に存在します。攻撃者がクライアントからTLSサーバへのトラフィックを代行受信できる場合、攻撃者は不正なTLSサーバをステージングしてそのトラフィックを代行受信し、クライアントが望ましいTLSサーバであると考えるものにクライアントを認証するように見える可能性があります。これにより、攻撃者は正規のTLSサーバに対して認証を行い、中間者攻撃を仕掛けることができます。ただし、攻撃者はセッションの内容を表示できず、データまたは要求を挿入することしかできません。

この脆弱性を不正利用するプルーフオブコンセプトコードが一般に公開されています。

OpenSSLは、この脆弱性をchangelogで確認し、更新されたソフトウェアをリリースしました。

この脆弱性を不正利用するには、攻撃者はTLSクライアントからTLSサーバへのトラフィックを代行受信できる必要があります。多くの場合、攻撃者はターゲットユーザのシステムに隣接するネットワークにアクセスする必要があります。また、攻撃者が正当なTLSサーバに隣接するネットワークにアクセスできる可能性もあります。

この脆弱性は、TLSの複数の実装に影響を与える可能性があります。

該当製品

Apacheは次のリンクでchangelogをリリースしました： Apache 2.2.15での変更

Appleは、 Security Update 2010-001、 Java for Mac OS X 10.6 Update 3、および Java for Mac OS X 10.5 Update 8の各リンクでセキュリティアップデートをリリースしています

シスコは、 cisco-sa-20091109-tlsのリンクでセキュリティアドバイザリを再リリースしました。このアドバイザリには関連するバグID番号が記載されていますが、これらの番号は製品に脆弱性が存在するか、または存在しないことが確認されると変更される可能性があります。

Citrixは次のリンクでセキュリティアドバイザリをリリースしました。 CTX123359

F5は次のリンクで登録ユーザ向けのセキュリティアドバイザリをリリースしています。 CVE-2009-3555

FreeBSDは次のリンクからセキュリティアドバイザリを公開しています。 FreeBSD-SA-09:15.ssl

FreeBSDは次のリンクでVuXMLドキュメントを公開しています。 mozilla – 複数の脆弱性

HPは次のリンクでセキュリティ情報をリリースしています。c01945686(HPSBUX02482 SSRT090249)、c02079216(HPSBUX02517 SSRT100058)、c02171256(HPSBMA02534 SSRT090180)、c02122104(HPSBUX02524 SSRT100089)、c02436041(HPSBGN02562 SSRT0949)、c02512995(HPSBMA02568 SSRT10) 0219、c02616748(HPSBUX02608 SSRT100333)、c03263573(HPSBMU02759 SSRT100817)、c03281831(HPSBOV02762 SSRT100825)。HPでは、 HPSBU02498 SSRT090264および HPSBMA02547 SSRT100179で、登録ユーザ向けのセキュリティ情報c01963123およびc02273751もリリースしています。

IBMは PK96157、 PM12247、および PM10658でAPARをリリースしました。IBMは次のリンクでアドバイザリをリリースしています：swg24025312、 swg21415080、 swg21426108、 swg24006386、および swg2160716。IBMは次のリンクでセキュリティアラートを再リリースしました： CVE-2009-3555。IBMは次のリンクで登録ユーザ向けのAPARをリリースしています。 IC68055

Microsoftは、 MS10-049、 Microsoft Security Advisory(977377)、および KB 977377の各リンクで、セキュリティ情報、セキュリティアドバイザリ、およびナレッジベース記事をリリースしています

MontaVistaソフトウェアは、2012年3月9日に登録ユーザに対するセキュリティアラートをリリースしました。このアラートは次のリンクで確認できます。 MontaVista Security Fixes

Mozillaは次のリンクでセキュリティアドバイザリをリリースしました。 MFSA 2010-22

NetBSDは次のリンクでセキュリティアドバイザリをリリースしています。 NetBSD-SA2010-002

Novellは次のリンクでセキュリティアドバイザリをリリースしました。 7005950

OpenBSDは次のリンクでセキュリティに関するアナウンスをリリースしています。 004：セキュリティ修正： 2009年11月26日および 010：セキュリティ修正： 2009年11月26日

OpenOffice.orgは、次のリンクでセキュリティ情報をリリースしています。 CVE-2009-3555

Oracleは次のリンクでセキュリティアラートをリリースしました。 Critical Patch Update March 2010

Red Hatはセキュリティアドバイザリを次のリンクでリリースしました： RHSA-2009:1579、RHSA-2009:1580、RHSA-2010:0011、RHSA-2010:0119、RHSA-2010:0130、RHSA-2010:055、RHSA-2010:0162、RHSA-2010:0163、RHSA-2010:0164、RHSA-2010:0165、RHSA-2010:0166、RHSA-2010:0167、RHSA-2010 0339、RHSA-2010:0408、RHSA-2010:0440、RHSA-2010:0770、RHSA-2010:0786、RHSA-2010:0807、RHSA-2010:0986、RHSA-2010:0 987

Sunは、 273029、 273350、および 274990の各リンクでセキュリティアドバイザリを再リリースしました

Sunは次のリンクでセキュリティ通知をリリースしました。 CVE-2009-3555

US-CERTは次のリンクで脆弱性に関するノートをリリースしました。 VU#120541

VMwareは、 VMSA-2010-0015および VMSA-2010-0019のセキュリティアドバイザリをリリースしました。

脆弱性のある製品

次の実装に脆弱性が存在します。

- バージョン0.9.8lより前のOpenSSLバージョン
- GnuTLSバージョン2.8.5以前

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

適切なアップデートを適用することを推奨します。

内部ネットワークを物理的に保護し、ハブではなくスイッチを使用してデータをルーティングすることを推奨します。

ファイアウォールとウイルス対策アプリケーションの両方を実行して、インバウンドとアウトバウンドの脅威の可能性を最小限に抑えることをお勧めします。

修正済みソフトウェア

OpenSSLは次のリンクで更新されたソフトウェアをリリースしました： openssl-0.9.8l.tar.gz

Apacheは次のリンクで更新されたソフトウェアをリリースしました： Apache HTTP Server 2.2.15

Appleは次のリンクで更新されたソフトウェアをリリースしています。
Mac OS XおよびMac OS X Server 10.6.4
セキュリティアップデート2010-001(Snow Leopard)
Java for Mac OS X 10.6 Update 3
Mac OS XおよびMac OS X Server 10.5.8
セキュリティアップデート2010-001クライアント(Leopard)
セキュリティアップデート2010-001サーバ(Leopard)
Java for Mac OS X 10.5 Update 8
CentOSパッケージは、 up2dateまたは yumコマンドを使用して更新できます。

F5は、次のリンクで登録ユーザ向けの更新されたソフトウェアをリリースしました。 F5 Products

FreeBSDはHTTPリンク ssl.patchでパッチを公開しています。

FreeBSDは次のリンクからportsコレクションの更新をリリースします。 Ports Collection Index

HPは次のリンクで更新されたソフトウェアをリリースしています。
x86
Linuxバージョン6.2用のHP System Managementホームページ
AMD64/EM64T
Linuxバージョン6.2用のHP System Managementホームページ

x86/x64
Windowsバージョン6.2用のHP System Managementホームページ
B.11.11 PA（32および64）
OpenSSL_A.00.09.08l.001
OpenSSL_A.00.09.08n.001_HP-UX_B.11.11_32+64.depot
Apache 2.0.59.13 PA-64-32-1111.depot

B.11.23（PAおよびIA）
OpenSSL_A.00.09.08l.002
OpenSSL_A.00.09.08n.002_HP-UX_B.11.23_IA-PA.depot
Apache 2.0.59.13 IA-PA-32-1123.depotです。
Apache 2.0.59.13 IA-PA-64-1123.depotです。

B.11.31（PAおよびIA）
OpenSSL_A.00.09.08l.003
OpenSSL_A.00.09.08n.003_HP-UX_B.11.31_IA-PA.depot
Apache 2.0.59.13 IA-PA-32-1131.depot
Apache 2.0.59.13 IA-PA-64-1131.depot

HP System Managementホームページ
v6.1.0.102以降（Windowsの場合）
v6.1.0-103以降（Linux x86用）
v6.1.0-103以降（Linux AMD64/EM64T用）

HP-UX B.11.31
JDKおよびJRE v6.0.07以降
JDKおよびJRE v5.0.20以降
SDKおよびJRE v1.4.2.25以降
JDKおよびJRE v6.0.09以降
JDKおよびJRE v5.0.21以降

HP-UX B.11.23
JDKおよびJRE v6.0.07以降
JDKおよびJRE v5.0.20以降
SDKおよびJRE v1.4.2.25以降
JDKおよびJRE v6.0.09以降
JDKおよびJRE v5.0.21以降

HP-UX B.11.11
JDKおよびJRE v6.0.07以降
JDKおよびJRE v5.0.20以降
SDKおよびJRE v1.4.2.25以降
JDKおよびJRE v6.0.09以降
JDKおよびJRE v5.0.21以降

HP Systems Insight Manager(SIM)
v6.1以降（HP-UX、Linux、Windows用）

HP ProCurve Threat Management Services zlモジュール

バージョンST.1.1.100430以降

CSWS_JAVA V3.2
HPは次のリンクで登録ユーザ向けの更新ソフトウェアをリリースしています。

HP Onboard Administrator 3.50
IBMは swg24025312および swg24006386の暫定的な修正をリリースしています。IBMは PK96157、 PM12247、および PM10658でAPARをリリースしました。IBM JDKのユーザは、JSSE APAR IZ65239をインストールすることをお勧めします。IBMは、 IBM developer kits、IBM DB2 version 9.1 Fix Pack 9、および IBM DB2 version 9.7 Fix Pack 2の各リンクでアップデートをリリースしています。
IBMは、 IBM Tivoli Endpoint Manager 8.2.1310 のリンクで修正をリリースしています。

Microsoftのお客様は、セキュリティ情報のリンクを使用して直接アップデートを入手できます。これらのアップデートはWindowsの自動更新機能によっても配布され、 Windows Update Webサイトで入手できます。Microsoft Windows Server Update Services (WSUS)、Systems Management Server、およびSystem Center Configuration Managerは、管理者がソフトウェア更新プログラムを展開する際に役立ちます。

MontaVistaソフトウェアは、次のリンクで更新されたソフトウェアをリリースしています。
PRO 5.0
Pro 5.0.24
Mobilinux 5.0.24
第5海抜
Pro 4.0.1
CGE 4.0.1
Mobilinux 4.1
Moblinux 4.0.2
CGE 5.1
Mobilinux 5.0
Mozillaは次のリンクで更新されたソフトウェアをリリースしています。
Firefox 3.6.2
Firefox 3.5.9
Thunderbird 3.0.4
SeaMonkey 2.0.4
NetBSDは次のリンクで利用可能なパッチをインストールする手順をリリースしました： NetBSD

OpenBSDは、 OpenBSD 4.5と OpenBSD 4.6のFTPリンクでソースコードのパッチをリリースしています

OpenOffice.orgでは、次のリンクで更新バージョンをリリースしています。 OpenOffice.org 3.2.1

Oracleは、登録ユーザ向けのパッチを次のリンクでリリースしました。 Oracle

Red Hatパッケージは、 up2dateまたは yumコマンドを使用して更新できます。
Sunは次のリンクでパッチをリリースしています。 SPARC

- パッチ 119209-22以降が適用されたSolaris 8
- パッチ 119211-22以降が適用されたSolaris 9
- Solaris 10(パッチ 119213-21以降)
- パッチ 125358-10以降が適用されたSun Java Enterprise System 5
- Sun Java System Web Server 7.0 update 7以降
- パッチ 125437-18以降が適用されたSun Java System Web Server 7.0
- Sun Java System Web Proxy Server 4.0.13以降
- Sun GlassFish Enterprise Server v2.1.1 with HADB – パッチ 128640-15以降（有効なサポート契約をお持ちのお客様の場合）または 141709-03以降（有効なサポート契約のないお客様の場合）
- パッチ 128643-15以降が適用されたHADBを搭載したSun GlassFish Enterprise Server v2.1.1（有効なサポート契約をお持ちのお客様の場合）または 141700-03（有効なサポート契約のないお客様の場合）
- パッチ 142806-02以降が適用されたSun Java System Directory Server 5.2 Patch 6
- パッチ 142807-02以降が適用されたSun Java System Directory Server Enterprise Edition 6.3.1

Intel

- パッチ 119212-22以降が適用されたSolaris 9
- Solaris 10(パッチ 119214-21以降)
- パッチ 125359-10以降が適用されたSun Java Enterprise System 5
- Sun Java System Web Server 7.0 update 7以降
- パッチ 125438-18以降が適用されたSun Java System Web Server 7.0
- Sun Java System Web Proxy Server 4.0.13以降
- Sun GlassFish Enterprise Server v2.1.1 with HADB – パッチ 128641-15以降（有効なサポート契約をお持ちのお客様の場合）または 141710-03以降（有効なサポート契約のないお客様の場合）
- パッチ 128644-15以降が適用されたHADBを搭載したSun GlassFish Enterprise Server v2.1.1（有効なサポート契約をお持ちのお客様の場合）または 141701-03（有効なサポート契約のないお客様の場合）
- パッチ 142806-02以降が適用されたSun Java System Directory Server 5.2 Patch 6
- パッチ 142807-02以降が適用されたSun Java System Directory Server Enterprise Edition 6.3.1

Linux

- パッチ 142506-03以降が適用されたSun Java Enterprise System 2005Q4およびSun Java

Enterprise System 5（RHEL2.1およびRHEL3.0用）
- パッチ 121656-21以降が適用されたSun Java Enterprise System 5（RHEL4.0およびRHEL5.0用）
- Sun Java System Web Server 7.0 update 7以降
- パッチ 125439-16以降が適用されたSun Java System Web Server 7.0
- パッチ 119171-33以降が適用されたSun Java System Application Server 8.1
- Sun Java System Web Proxy Server 4.0.13以降
- Sun GlassFish Enterprise Server v2.1.1 with HADB – パッチ 128642-15以降（有効なサポート契約をお持ちのお客様の場合）または 141711-03以降（有効なサポート契約のないお客様の場合）
- パッチ 128645-15以降が適用されたHADBを搭載したSun GlassFish Enterprise Server v2.1.1（有効なサポート契約をお持ちのお客様の場合）または 141702-03（有効なサポート契約のないお客様の場合）
- パッチ 142806-02以降が適用されたSun Java System Directory Server 5.2 Patch 6
- パッチ 142807-02以降が適用されたSun Java System Directory Server Enterprise Edition 6.3.1

HP-UX

- パッチ 124379-12以降が適用されたSun Java Enterprise System 2005Q4およびSun Java Enterprise System 5
- Sun Java System Web Server 7.0 update 7以降
- パッチ 125440-16以降が適用されたSun Java System Web Server 7.0
- Sun Java System Web Proxy Server 4.0.13以降
- パッチ 142806-02以降が適用されたSun Java System Directory Server 5.2 Patch 6
- パッチ 142807-02以降が適用されたSun Java System Directory Server Enterprise Edition 6.3.1

Windows

- パッチ 124392-11以降が適用されたSun Java Enterprise System 2005Q4
- パッチ 125923-10 以降が適用されたSun Java Enterprise System 5
- Sun Java System Web Server 7.0 update 7以降
- パッチ 125441-18以降が適用されたSun Java System Web Server 7.0
- パッチ 119172-33以降が適用されたSun Java System Application Server 8.1
- Sun Java System Web Proxy Server 4.0.13以降
- パッチ 128646-15以降が適用されたHADBを搭載したSun GlassFish Enterprise Server v2.1.1（有効なサポート契約をお持ちのお客様の場合）または 141703-03（有効なサポート契約のないお客様の場合）
- パッチ 142806-02以降が適用されたSun Java System Directory Server 5.2 Patch 6
- パッチ 142807-02以降が適用されたSun Java System Directory Server Enterprise Edition 6.3.1

AIX

- パッチ142806-02以降が適用されたSun Java System Directory Server 5.2 Patch 6

Sunは次のリンクで、関連するプラットフォーム向けのStarOffice/StarSuite用パッチをリリースしました： CVE-2009-3555

VMwareは、次のリンクで更新されたソフトウェアをリリースしています。
ESX 3.5
ESX350-201012401-SG
ESX 4.0
ESX400-201009401-SG
ESX 4.1
ESX410-201010402-SG

推奨事項

$propertyAndFields.get("recommendations")

不正利用事例と公式発表

Cisco Product Security Incident Response Team（PSIRT）は、本アドバイザリに記載されている脆弱性の不正利用事例やその公表を確認していません。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/Cisco-SA-20091105-CVE-2009-3555

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.0	初版リリース	適用外	Final	2009年11月5日

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。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。