Transport Layer Security 再ネゴシエーション リモート Man-in-the-middle攻撃脆弱性

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 :** Yes **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

複数の Transport Layer Security （ TLS ）実装は非認証を可能にする可能性がある man-in-the-middle攻撃を行なうために TLS セッションを再取り決めするときリモート攻撃者脆弱性が含まれています。

TLS 再ネゴシエーション プロセスの間に存在 する脆弱性。 攻撃者がクライアントから TLS サーバにトラフィックを代行受信できる場合攻撃者はそのトラフィックを代行受信するために不正な TLS サーバを上演する可能性があり、クライアントを認証するようであるクライアントが考えるものをへの望ましい TLS サーバです。 攻撃者は正規の TLS にサーバを認証し、こうして man-in-the-middle攻撃を上演それからできます。 ただし、攻撃者はセッションのコンテンツを表示できなかったし、それにデータか要求をインジェクトためにだけできます。

この脆弱性を不正利用するプルーフ オブ コンセプト コードは共用利用可能です。

OpenSSL は changelog のこの脆弱性を確認し、更新済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ために、攻撃者は TLS クライアントから TLS サーバに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、これは攻撃者がターゲットとされたユーザのシステムに隣接してあるネットワークにアクセスできるように要求するかもしれません。 もう一つの可能性は正規の TLS サーバに隣接してあるネットワークにアクセスできる攻撃者のためです。

この脆弱性は可能性が高いです TLS の複数の実装に影響を与える。

該当製品

修正済みソフトウェア

次の実装は脆弱です:

- バージョン 0.9.8l 以前の OpenSSL バージョン
- GnuTLS バージョン 2.8.5 および前に

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。

改訂履歴

バージョン	説明	Section	ステータス	日付
1.0	初版リリース	該当なし	Final	2009-Nov-05

利用規約