Cisco PIX/ASA DHCP リレー エージェント メモリリーク の 脆弱性

Medium	**アドバイザリーID :** Cisco-SA-20070502-CVE-2007-2461 **初公開日 :** 2007-05-02 18:25 **バージョン 1.0 :** Final **CVSSスコア :** 2.7 **回避策 :** Yes **Cisco バグ ID :**	CVE-2007-2461

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

Cisco により PIX 適応型セキュリティ アプライアンス (ASA) ソフトウェア (ASA) ソフトウェア バージョン 7.2(1) ～ 7.2(2.14) 非認証を可能にする可能性がある影響を受けたデバイスはトラフィックを転送することを止めます脆弱性がリモート攻撃者含まれ。

特定の DHCP パケットをある特定のコンフィギュレーションの下で処理する場合の エラーによるこの脆弱性存在。 非認証はトラフィックを処理するための利用可能なメモリ メモリ· リソースを消費しますデバイスは影響を受けたデバイスによりへ多数の DHCP 要求を送信 することによって、リモート攻撃者この脆弱性を不正利用する可能性があります。 デバイスは利用可能なメモリを排出するとき、サービス拒否 (DoS) 状態に終ってトラフィックを、転送し終えます。

Cisco はこの脆弱性およびリリースされたソフトウェア アップデートを確認しました。

この脆弱性を不正利用するために、複数の DHCPサーバに DHCPリレーで設定される影響を受けたデバイスとして同じ サブネットにある攻撃者はシステムを制御する必要があります。 脆弱性は正当 な Clients 要求 DHCP リース、そう結局影響を受けた PIX または ASA デバイスがトラフィックを転送し終えるので、それ自身を通常の状態でゆっくり明示します。 ただし、脆弱 な 設定の脆弱 な デバイスとのサブネットへのアクセスの攻撃者によりすぐに影響を受けたデバイスは繰り返された DHPC 要求によってトラフィックを転送することを止めます場合があります。 しかし後最初の要求が、攻撃者のシステム DHCPリースを許可された。 この脆弱性を不正利用する追加要求をするために、攻撃者はシステムのネットワーク カードの MAC アドレスを変え、次に New 要求をする必要があります。 これは可能性のあるですが、使用されるオペレーティング

システムによっていくつかのスキルか特別なツールを、必要とします。　それは何時間が影響を受けたメモリスペースをいっぱいにする DHCP 要求をすることを攻撃者は必要とするか丁度明白でないです; ただし、DHCPリース 割り当ての各例はデバイスのパフォーマンスを低下させます。

ユーザはまだコンソールポートにデバイスがパケットを転送し終えたら管理者接続する可能性がありますシステムをリブートするか、または他の管理行為を行うためにそれに注意する必要があります。

DHCPリレーは影響を受けたデバイスでデフォルトで設定されません。

Firewall Services Module（FWSM）はこの脆弱性から影響を受けません。

該当製品

修正済みソフトウェア

Cisco PIX/ASA ソフトウェア バージョンは 7.2(1) 〜 7.2(2.14) 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。

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	2007 年 5 月 2 日

利用規約