Cisco PIXおよびASAアプライアンスのDHCPリレーエージェントの脆弱性

Informational

アドバイザリーID : cisco-sa-20070502-pix
初公開日 : 2007-05-02 16:00
バージョン 1.0 : Final
回避策 : No Workarounds available
Cisco バグ ID :

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

これは、2007年5月2日に公開された「Cisco ASA fails to properly process DHCP relay packets」というタイトルのCERT/CCアドバイザリに対するシスコの回答です。このアドバイザリは次のリンクで確認できます。http://www.kb.cert.org/vuls/id/530057

シスコは、CERT/CCによって公開されたアドバイザリに従ってメモリ枯渇の脆弱性を確認し、この脆弱性がPIXおよびASAアプライアンスに影響を与えるのはシステムソフトウェア7.2のみであることを確認します。この脆弱性が不正利用されると、アプライアンスに対するDenial of Service(DoS)状態が発生する可能性があります。

ファイアウォールサービスモジュール(FWSM)は、この脆弱性の影響を受けません。

PSIRTは、この脆弱性をシスコに報告していただいたCERT/CCのGrant Deffenbaugh氏とLisa Sittler氏に感謝いたします。

シスコは、研究者と協力してセキュリティ脆弱性に関する調査を行い、シスコ製品に対するセキュリティ脆弱性レポートの作成を支援する機会を得たことを非常に感謝しています。

追加情報

DHCPプロトコルは、IPアドレス、サブネットマスク、デフォルトゲートウェイ、DNSサーバアドレス、WINSアドレスなどの自動設定パラメータをホストに提供します。最初は、DHCP クライアントにこれらの設定パラメータはありません。DHCP クライアントは、設定パラメータのブロードキャスト要求を送信して、この情報を取得します。DHCP サーバがこの要求を見て、必要な情報を提供します。ルータやファイアウォールなどのレイヤ 3 デバイスは、一般に、デフォル

トではこれらのブロードキャスト要求を転送しません。

DHCPクライアントとDHCPサーバを同じサブネット上に配置するのが不便な状況では、PIXとASAのセキュリティアプライアンスがDHCPリレーメカニズムを使用する手段を提供します。DHCPリレーエージェントは、設定されているリスニングインターフェイス上でDHCPクライアントから最初のDHCPDISCOVERブロードキャストメッセージを受信すると、別の設定されているインターフェイス上に配置されている指定されたDHCPサーバすべてに要求を転送します。DHCPサーバはDHCPOFFERメッセージで応答します。DHCPリレーエージェントはこれを元のDHCPクライアントに転送します。次に、DHCPクライアントはDHCPREQUESTブロードキャストメッセージで応答し、特定のDHCPプロポーザルを選択します。このプロポーザルは、DHCPリレーエージェントによってすべてのDHCPサーバに転送されます。選択したリースを持つDHCPサーバは、DHCPリレーエージェントによって転送されるDHCPACKを返して、リースが確定したことをDHCPクライアントに通知します。

クライアントが他の手段（手動設定など）でネットワークアドレスを取得した場合は、DHCPINFORM要求メッセージを使用して、他のローカル設定パラメータを取得できます。このパラメータは、DHCPリレーエージェントによってすべてのDHCPサーバに転送されます。DHCPINFORMを受信したDHCPサーバは、クライアントに適したローカル設定パラメータを含むDHCPACKメッセージを返します。このパラメータもDHCPリレーエージェントによって転送されます。

したがって、DHCPリレーエージェントは、DHCPサーバとの通信においてDHCPクライアントのプロキシとして機能します。

DHCPリレーエージェント機能を使用するように設定されている場合、PIXおよびASAアプライアンスシステムソフトウェアに脆弱性が存在します。この脆弱性では、DHCPクライアントのDHCPREQUESTまたはDHCPINFORMメッセージに対する応答として複数のDHCPサーバからDHCPACKメッセージを受信すると、1550バイトのブロックメモリ（セキュリティアプライアンスでの処理用のイーサネットパケット）が格納に使用)がされる原因になる場合があります。これは、該当するバージョンが**dhcprelay server**コマンドを使用して複数のDHCPサーバで設定されている通常のデバイスの動作中に発生する可能性があります。1550バイトのブロックメモリが完全に使い果たされると、アプライアンスはパケットの廃棄を開始し、パケットが転送されなくなります。**dhcprelay server**コマンドで単一のDHCPサーバだけを設定したシステムには、脆弱性はありません。

この脆弱性は、Cisco Bug ID CSCsh50277(登録ユーザ専用)に記載されています。

この脆弱性は、システムソフトウェアバージョン7.2(1)から7.2(2.14)に影響を与えます。

シスコは、次の場所からダウンロードできる修正済みシステムソフトウェア(7.2(2.15)以降)を提供しています。

- ASA:http://www.cisco.com/pcgi-bin/tablebuild.pl/asa-interim
- PIX:http://www.cisco.com/pcgi-bin/tablebuild.pl/pix-interim

PIXまたはASAアプライアンスがDHCPリレーエージェント機能を使用するように設定されているかどうかを確認するには、アプライアンスにログインして、コマンドラインインターフェイス

(CLI)コマンドshow dhcprelay stateを発行します。「DHCP用に設定されていません」以外の情報を返すシステムには脆弱性が存在します。または、アプライアンスにログインし、CLIコマンドshow running-config dhcprelayを発行します。

次の例は、DHCPリレーエージェント用に設定されていないアプライアンスを示しています。

```
pix#show dhcprelay state
Context  Not Configured for DHCP
Interface outside, Not Configured for DHCP
Interface inside, Not Configured for DHCP
pix#

asa#show dhcprelay state
 Not Configured for DHCP
asa#
```

次の例は、DHCPリレーエージェント用に設定されたアプライアンスを示しています。

```
asa#show dhcprelay state
Context  Configured as DHCP Relay
Interface outside, Configured for DHCP RELAY
Interface inside, Configured for DHCP RELAY SERVER
asa#
```

次の例は、show running-config CLIコマンドを使用して、DHCPリレーエージェント用に設定されたアプライアンスの確認を示しています（DHCPリレーエージェント用に設定されていないアプライアンスは何も返しません）。

```
asa#show running-config dhcprelay
dhcprelay server 10.2.1.2 outside
dhcprelay enable inside
dhcprelay timeout 60
asa#
```

次の例は、DHCPリレーエージェントが設定されていないアプライアンスからの応答を示しています。

```
asa#show running-config dhcprelay
asa#
```

回避策

この脆弱性に対する回避策はありません。

dhcprelay serverコマンドで単一のdhcprelayサーバが設定されている場合は、この脆弱性が通常の動作条件下で見られるのを防ぐことができます。

次に、2台のdhcprelayサーバが設定された状態で稼働し、緩和策を適用しているシステムの例を示します。

```
asa#show running-config dhcprelay
dhcprelay server 192.168.200.210 inside
dhcprelay server 192.168.200.200 inside
dhcprelay enable outside
dhcprelay timeout 60
asa(config)#no dhcprelay server 192.168.200.210 inside
asa(config)#exit
asa#
asa#show running-config dhcprelay
dhcprelay server 192.168.200.200 inside
dhcprelay enable outside
dhcprelay timeout 60
asa#
```

dhcprelay serverコマンドまたは**dhcprelay enable**が設定されていないインターフェイスで受信されたDHCPパケットは、ファイアウォールによって廃棄されます。

ネットワーク環境に応じて、ACLの使用や、インフラストラクチャACL(iACL)またはユニキャストReverse Path Forwarding（ユニキャストRPF）の形式でのアンチスプーフィング保護の実装によって、「dhcprelay server」コマンドが設定されたインターフェイスの背後にある送信元からの悪意のある不正使用の可能性がさらに軽減されます。iACLの詳細については、『コアの保護：インフラストラクチャ保護ACL』を参照してください。

ユニキャストRPFの詳細については、IETF Best Current Practice 84「Ingress Filtering for Multihomed Networks」を参照してください。http://www.ietf.org/rfc/rfc3704.txt

シスコのセキュリティ手順

シスコ製品のセキュリティの脆弱性に関するレポート、セキュリティ障害に対する支援、およびシスコからのセキュリティ情報を受信するための登録に関するすべての情報は、シスコのワールドワイド ウェブサイト https://sec.cloudapps.cisco.com/security/center/resources/security_vulnerability_policy.html から入手できます。この情報には、シスコのセキュリティ通知に関して、報道機関が問い合せる場合の説明も含まれています。すべての Cisco セキュリティ アドバイザリは、http://www.cisco.com/go/psirt から入手できます。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070502-pix

改訂履歴

バージョン	説明	セクション	日付
リビジョン 1.0	初版リリース		2007 年 5 月 2 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。