Internet Key Exchange Protocolバージョン1におけるサービス妨害の脆弱性

Medium

アドバイザリーID : Cisco-SA-20060726-CVE-2006-3906　[CVE-2006-3906]

初公開日 : 2006-07-26 22:36

最終更新日 : 2015-01-31 08:30

バージョン 3.0 : Final

CVSSスコア : 2.3

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

複数の製品に、インターネットキーエクスチェンジ(IKE)バージョン1プロトコルの実装の脆弱性が存在します。 IKEは通常、IPSecでのキー交換に使用され、IPSecは通常、VPN接続のデータの暗号化に使用されます。

この脆弱性は、メインモードとアグレッシブモードの両方でIKEフェーズ1ネゴシエーションに影響します。 この脆弱性は、通常のUDPベースのIKEと、シスコ独自のTCPカプセル化IKEに影響を与えます。この脆弱性は、システムに送信される大量のIKE要求の不適切な処理に起因します。 該当するデバイスでは、IKEセッションに対する最初の要求が要求キューがいっぱいになる前に、それらの要求をキューに入れることしかできません。 攻撃者は、この脆弱性を不正利用して、デバイスがキューから期限切れになるよりも早く多数のIKEセッションを開始することで、IKEリソースを枯渇させる可能性があります。 このアクションにより、攻撃者がパケットの送信を停止するまでデバイスはIKE要求を処理できないため、サービス拒否(DoS)状態が発生します。

この脆弱性は確認されていますが、アップデートは提供されていません。

このエラーは認証の前に発生するため、攻撃者がこの脆弱性を不正利用するために有効なクレデンシャルは必要ありません。 この脆弱性の不正利用に使用されるIKEパケットは有効であり、この不正利用に必要なパケットのレートは比較的低いため、IDSおよびIPSシステムは攻撃を検出できない可能性があります。 この攻撃では高い帯域幅は必要ありません。これにより、攻撃者は複数のデバイスをターゲットにすることができます。 ただし、帯域幅を増やすと、IDSまたはIPSに

よる攻撃の検出が容易になります。 攻撃者は、送信元IPアドレスのスプーフィングをUDP経由で使用して攻撃元を偽装し、進行中の攻撃のブロックをより困難にすることができます。

この脆弱性は主にインターネットに公開されているVPNアプライアンスに影響を与えるため、脆弱なシステムのIPアドレスにアクセスできるユーザであれば攻撃を仕掛けることができます。 攻撃者は、ポートスキャンと組み合わせてOSフィンガープリントを使用して、脆弱なシステムを検出する可能性があります。

この脆弱性は、さまざまな製品に影響を与える可能性があります。 Cisco IOSソフトウェア、VPN 3000シリーズコンセントレータ、PIXおよびASAセキュリティアプライアンスには脆弱性が存在します。

該当製品

シスコでは、Cisco Bug ID CSCse70811、CSCse89808、CSCsb51032、CSCse92254、CSCse92527、およびCSCse96516に対応するセキュリティ応答を次のリンクで再リリースしています。Cisco-sr-20060726

脆弱性のある製品

オペレーティングシステム、ファイアウォール、またはVPNアプライアンスにIKEバージョン1を実装しているシステムには、脆弱性が存在する可能性があります。

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、将来のアップデートやリリースについてベンダーに問い合わせることをお勧めします。

ネットワークに脆弱性が存在する可能性のあるアプライアンスまたはシステムがないかどうかを確認することを推奨します。

管理者は、それぞれの状況に固有の回避策についてベンダーに問い合わせることを推奨します。

ACLを使用して、該当するデバイスへのIKEトラフィックを制限することが推奨されます。

管理者は、該当するデバイスがバージョン1ではなくIKEプロトコルバージョン2を使用するように設定できます。

管理者は、攻撃が進行中であることを示す可能性がある大量のIKEパケットを監視するようにIPSまたはIDSシステムを設定することを推奨します。

Cisco IOSをご使用のお客様は、IKEのコールアドミッション制御機能を実装することで、この脆弱性を緩和できます。

個々の製品の緩和戦略に関するシスコの詳細は、次のリンク先で参照できます。Cisco

修正済みソフトウェア

パッチおよびソフトウェアアップデートは利用できません。

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-20060726-CVE-2006-3906

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	2006年7月26日

利用規約

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。