Cisco ASAソフトウェアのVPNグループの列挙に関する脆弱性

アドバイザリーID : Cisco-SA-20130418-CVE-2013-1194

CVE-2013-1194

初公開日 : 2013-04-18 14:22

バージョン 1.0 : Final

CVSSスコア : 5.0

回避策 : No Workarounds available

Cisco バグ ID : CSCue73708

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適応型セキュリティアプライアンス(ASA)ソフトウェアのInternet Security Association and Key Management Protocol(ISAKMP)実装における脆弱性により、認証されていないリモートの攻撃者が、Cisco ASAデバイスで設定されているリモートアクセスVPNグループを列挙できる可能性があります。

この脆弱性は、有効および無効なVPNグループがAM1メッセージに含まれている場合に、Cisco ASAソフトウェアがインターネットキーエクスチェンジ(IKE)アグレッシブモードメッセージに応答する方法が異なることに起因します。攻撃者は、VPNヘッドエンドとして設定されているCisco ASAデバイスに巧妙に細工されたIKEメッセージを送信することで、この脆弱性を不正利用する可能性があります。

この脆弱性は、Trustwave SpiderLabsのDaniel Turner氏によって発見されました。この問題を報告いただき、弊社と連携しての公開にご協力いただいたTrustwave SpiderLabsに感謝いたします。

シスコは、セキュリティ通知の脆弱性とソフトウェアアップデートが利用可能であることを確認しました。

この脆弱性を不正利用するには、攻撃者が信頼できる内部ネットワークにアクセスし、巧妙に細工されたIKEメッセージをターゲットシステムに送信する必要があります。このアクセス要件により、攻撃が成功する可能性が低くなる可能性があります。

影響を受けるバージョンの最新リストについては、ベンダーアナウンスセクションのバグレポートを参照してください。

シスコはCVSSスコアを通じて、機能的なエクスプロイトコードが存在することを示していますが、このコードが一般に公開されることは確認されていません。

該当製品

シスコは、次のリンクでバグID CSCue73708のセキュリティ通知をリリースしています。 CVE-2013-1194

脆弱性のある製品

このアラートが最初に発行された時点では、Cisco ASAソフトウェアバージョン9.1.2以前には脆弱性が存在していました。Cisco ASAソフトウェアの新しいバージョンも影響を受け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

適切なアップデートを適用することを推奨します。

ネットワークデバイスへの不正な直接通信を防止することが重要です。偵察攻撃やDoS攻撃から保護するために、ネットワークインフラストラクチャ宛てのネットワークトラフィックを制限します。設定の詳細については、『 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。

管理者は、堅実なファイアウォール戦略を使用して、影響を受けるシステムを外部の攻撃から保護できます。

管理者は、IPベースのアクセスコントロールリスト(ACL)を使用して、信頼できるシステムだけが該当システムにアクセスできるようにすることを検討できます。

影響を受けるシステムを監視することを推奨します。

修正済みソフトウェア

契約が有効なシスコのお客様は、シスコのサポートチームに連絡して、この脆弱性の修正を含むソフトウェアバージョンへのアップグレードの支援を受ける必要があります。契約をご利用でないお客様は、1-800-553-2447または1-408-526-7209のCisco Technical Assistance Center(TAC)にお問い合わせいただくか、 tac@cisco.comの電子メールでサポートを受けることができます。

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-20130418-CVE-2013-1194

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	2013年4月18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。