Cisco ASA 1000Vクラウドファイアウォール H.323インスペクションに関するDoS脆弱性

High

アドバイザリーID : cisco-sa-20130116-asa1000v
初公開日 : 2013-01-16 16:00
バージョン 1.0 : Final
CVSSスコア : 7.8
回避策 : No Workarounds available
Cisco バグ ID : CSCuc88741 CSCuc42812

CVE-2012-5419

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 ASA 1000Vクラウドファイアウォール用のCisco適応型セキュリティアプライアンス(ASA)ソフトウェアの脆弱性により、Cisco ASA 1000Vで不正なH.323メッセージが処理された後にリロードが発生する可能性があります。H.323インスペクションが有効な場合、Cisco ASA 1000Vクラウドファイアウォールが影響を受けます。

シスコはこの脆弱性に対処するソフトウェアアップデートをリリースしています。

このアドバイザリは次のリンクに掲載されます:

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130116-asa1000v

注：このアドバイザリに記載されている脆弱性の影響を受けるのは、Cisco ASA 1000Vクラウドファイアウォール用のCisco ASAソフトウェアのみです。Cisco ASA 5500シリーズ適応型セキュリティアプライアンス、Cisco Catalyst 6500シリーズASAサービスモジュール、またはCisco Catalyst 6500シリーズFirewall Services Module(FWSM)は、この脆弱性の影響を受けません。

該当製品

脆弱性のある製品

H.323インスペクションが有効になっている場合、Cisco ASA 1000Vクラウドファイアウォー

ル用のCisco ASAソフトウェアのバージョン8.7.1および8.7.1.1がこの脆弱性の影響を受けます。H.225およびRegistration, Admission and Status(RAS)メッセージに対するH.323インスペクションは、デフォルトで有効になっています。

この脆弱性は、H.225メッセージに対するH.323インスペクションが有効になっている場合にのみ存在します。 RASメッセージに対するH.323インスペクションは、この脆弱性には影響しません。

H.323 H.225インスペクションが有効になっているかどうかを判断するには、 show service-policy inspect h323 h225コマンドを発行して、クラスマップがH.225インスペクションエンジンで設定されていることを確認します。H.225メッセージのH.323インスペクションが設定されている場合、関連するH.323出力は参照先のクラスマップの下に表示されます。

次に出力例を示します。

```
ASA1000v# show service-policy inspect h323 h225
Global policy:
  Service-policy: global_policy
    Class-map: inspection_default
      Inspect: h323 h225 _default_h323_map, packet 0, lock fail 0, drop 0, reset-drop 0
               tcp-proxy: bytes in buffer 0, bytes dropped 0
        h245-tunnel-block drops 0 connection
```

注：上記の出力は、H.225メッセージに対するH.323インスペクションが適用されたクラスマップを持つポリシーマップを示しています。

または、H.225メッセージに対するH.323インスペクションが有効になっているデバイスは、次のような設定になっています。

```
class-map inspection_default
 match default-inspection-traffic
!
policy-map global_policy
 class inspection_default
  ...
  inspect h323 h225
  ...
!
service-policy global_policy global
```

注：上の例はグローバルアプリケーションを示していますが、サービスポリシーは特定のインターフェイスにも適用できます

Cisco Adaptive Security Device Manager(ASDM)を使用してデバイスを管理している場合は、

グローバルポリシーまたはインターフェイス固有のポリシーの下の サービスポリシーセクションをチェックして、インスペクションが有効になっているかどうかを判断できます。

Cisco Virtual Network Management Center(VNMC)を使用して複数のデバイスを管理している場合は、 Policy Management > Security Policies > Root > Tenant > Data Center > Policiesの下の Packet Inspectionセクションで、インスペクションが有効になっているかどうかを確認できます。
実行中のCisco ASA 1000Vクラウドファイアウォール用のCisco ASAソフトウェアのバージョンを確認するには、Cisco ASA 1000Vコマンドラインから show versionコマンドを発行します。

次の例は、該当するソフトウェアバージョン(8.7.1)を実行しているシステムを示しています。

```
ASA1000v(config)# show version
Cisco Adaptive Security Appliance Software Version 8.7(1)
Device Manager Version 6.3(5)
```

Cisco Adaptive Security Device Manager（ASDM）を使用してデバイスを管理している場合は、ログイン ウィンドウの表、または ASDM ウィンドウの左上にソフトウェアのバージョンが表示されます。

または、VMware vCenter ServerのCisco ASA 1000V Cloud FirewallリソースのSummaryタブからバージョン情報を取得することもできます。

脆弱性を含んでいないことが確認された製品

Cisco ASA 1000Vクラウドファイアウォールを除き、この脆弱性の影響を受けるシスコ製品は現在確認されていません。

詳細

Cisco ASA 1000Vクラウドファイアウォールは、マルチテナントのプライベートおよびパブリッククラウド環境におけるテナントエッジを保護する仮想セキュリティアプライアンスです。
VMware vSphere HypervisorソフトウェアとCisco Nexus 1000Vシリーズスイッチでのみ動作します。

Cisco ASA 1000Vクラウドファイアウォールは、仮想データセンター内の仮想マシン(VM)がインターネットに安全にアクセスできるようにし、VMのデフォルトゲートウェイとして機能し、ネットワークベースの攻撃から保護します。

1000V Cloud Firewallバージョン8.7.1および8.7.1.1用のCisco ASAソフトウェアには、認証されていないリモートの攻撃者がCisco 1000V Cloud Firewallのリロードを引き起こす可能性のある脆弱性が存在します。

この脆弱性は、不正なH.323パケットの不適切な処理に起因します。攻撃者は、該当デバイスを介して巧妙に細工されたH.323パケットを送信することにより、この脆弱性を不正利用する可能性があります。この不正利用により、攻撃者はCisco ASA 1000Vクラウドファイアウォールをリロードし、サービス妨害(DoS)状態を引き起こす可能性があります。

H.323through-the-boxトラフィックを検査するように設定されているCisco ASA 1000Vデバイスは、不正なH.323 IPv4パケットを受信するとリロードする可能性があります。

H.323制御チャネルは、H.225、H.245、およびH.323 RASメッセージを処理します。H.323検査では、次の既定のポートを使用します。

1718：ゲートキーパーディスカバリUDPポート
1719：RAS UDP ポート
1720：TCP 制御ポート

H.323コールシグナリングの設定手順の際に、追加のダイナミックUDPポートとダイナミックTCPポートがネゴシエートされる場合があります。

H.323インスペクションで使用される既知のポート、またはH.323コールシグナリング設定で動的にネゴシエートされるポートのいずれかに送信される不正なパケットがこの脆弱性を引き起こす可能性があります。

この脆弱性は、through-the-boxトラフィックによってのみ引き起こされます。Cisco ASA 1000Vクラウドファイアウォールは、H.225メッセージに対するH.323インスペクションが有効になっている場合にのみ影響を受けます。

Cisco ASA 1000Vクラウドファイアウォールは、IPv6トランスポート上でのH.323インスペクションをサポートしていません。

この脆弱性は、Cisco Bug ID CSCuc42812(登録ユーザ専用)および CSCuc88741(登録ユーザ専用)として文書化され、CVE-2012-5419が割り当てられています。

回避策

H.323インスペクションが不要な場合は、無効にして、デバイスが脆弱性の影響を受けないようにすることができます。管理者は、ポリシーマップ設定のクラス設定サブモードで no inspect h323 h225コマンドを発行することにより、H.225メッセージに対するH.323検査を無効にできます。回避策を有効にするには、H.225メッセージに対するH.323検査を無効にする必要があります。

次の例は、デフォルトのポリシーマップからH.323インスペクションを無効にする方法を示しています。

```
ASA1000v(config)# policy-map global_policy
ASA1000v(config-pmap)# class inspection_default
ASA1000v(config-pmap-c)# no inspect h323 h225
```

H.225メッセージに対するH.323検査が必要な場合は、回避策はありません。

修正済みソフトウェア

ソフトウェアのアップグレードを検討する場合は、 http://www.cisco.com/go/psirt の Cisco Security Advisories and Responses アーカイブや後続のアドバイザリを参照して、侵害を受ける可能性と完全なアップグレード ソリューションを確認してください。

いずれの場合も、アップグレードするデバイスに十分なメモリがあること、および現在のハードウェアとソフトウェアの構成が新規リリースで引き続き正しくサポートされていることを十分に確認してください。不明な点については、Cisco Technical Assistance Center（TAC）もしくは契約しているメンテナンスプロバイダーにお問い合わせください。

この脆弱性は、Cisco ASA 1000Vクラウドファイアウォールバージョン8.7.1.3以降のCisco ASAソフトウェアで修正されています。

Cisco ASA 1000Vクラウドファイアウォール用のCisco ASAソフトウェアは、次のリンクからダウンロードできます。

http://software.cisco.com/download/type.html?mdfid=284145419&catid=null

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。

この脆弱性は内部テストで発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130116-asa1000v

改訂履歴

リビジョン 1.0	2013年1月16日	初回公開リリース

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。