Cisco適応型セキュリティアプライアンスのアクセスコントロールリストにおけるICMPエコー要求コードフィルタリングの脆弱性

Medium	**アドバイザリーID :** cisco-sa-20160711-asa **初公開日 :** 2016-07-11 09:30 **最終更新日 :** 2016-07-21 20:44 **バージョン 1.1 :** Final **CVSSスコア :** 4.3 **回避策 :** No workarounds available **Cisco バグ ID :** CSCuy25163	CVE-2016-1445

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)ソフトウェアにおけるICMPエコー応答メッセージに対するアクセスコントロールリスト(ACL)の許可および拒否フィルタの実装の脆弱性により、認証されていないリモートの攻撃者が該当デバイスのACL設定をバイパスできる可能性があります。拒否する必要があるICMPトラフィックが、代わりに該当デバイスを通過することを許可される場合があります。

この脆弱性は、ICMPエコー要求に対するACLベースのフィルタの実装と、ICMPエコー要求サブタイプの範囲に起因します。攻撃者は、該当デバイスにICMPエコー要求トラフィックを送信することで、この脆弱性を不正利用する可能性があります。エクスプロイトに成功すると、攻撃者はデバイスのACL設定をバイパスし、代わりに拒否する必要があるトラフィックをデバイス経由で許可できる可能性があります。

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。この脆弱性に対処する回避策はありません。

このアドバイザリは次のリンクで確認できます。
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160711-asa

該当製品

脆弱性のある製品

Cisco適応型セキュリティアプライアンス(ASA)ソフトウェアリリース8.2から最初の修正済みソフトウェアリリースまでは、脆弱性が存在します。この脆弱性は、ソフトウェアバージョン9.4.3.3、9.5.2.10、および9.6.1.5で修正されています。修正済みリリースの詳細については、「修正済みソフトウェア」セクションを参照してください。

ASAは、ICMPエコー要求を許可するACLで設定されている場合に脆弱です。脆弱性のある設定の例を次に示します。

access-list my-list extended permit icmp any any echo-reply 0 log interval 1

Firepower Threat Defense(FTD)にも脆弱性が存在します。

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

この脆弱性に対処する回避策はありません。

修正済みソフトウェア

シスコでは、Cisco Bugsの修正済みソフトウェアに関する情報を提供しています。この情報には、 Cisco Bug Search Toolからアクセスできます。

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は新規リリースでも継続して適切なサポートが受けられることを確認してください。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。

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-

20160711-asa

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.1	脆弱性のある製品を明確にした。脆弱性のある設定を特定する手順を追加。	脆弱性が存在する製品	Final	2016年7月21日
1.0	初回公開リリース	-	Final	2016年7月11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。