Cisco Firepowerのマルウェアブロックバイパスの脆弱性

High

アドバイザリーID : cisco-sa-20160330-fp　CVE-2016-1345
初公開日 : 2016-03-30 16:00
バージョン 1.0 : Final
CVSSスコア : 5.0
回避策 : No workarounds available
Cisco バグ ID : CSCux22726

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 Firepowerシステムソフトウェアの悪意のあるファイルの検出とブロックの機能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該当システムのマルウェア検出メカニズムをバイパスできる可能性があります。

この脆弱性は、HTTPヘッダーのフィールドの不適切な入力検証に起因します。攻撃者は、該当システムに巧妙に細工された HTTP 要求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。エクスプロイトに成功すると、攻撃者は悪意のあるファイルの検出をバイパスしたり、システムに設定されたポリシーをブロックしたりして、マルウェアが検出されずにシステムを通過す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-20160330-fp

該当製品

脆弱性のある製品

この脆弱性は、1つ以上のファイルアクションポリシーが設定され、次のシスコ製品のいずれかで実行されているCisco Firepowerシステムソフトウェアに影響を与えます。

- FirePOWER サービスを使用する適応型セキュリティ アプライアンス（ASA）5500-X シ

リーズ
- ネットワーク向け Advanced Malware Protection（AMP）7000 シリーズ アプライアンス
- ネットワーク向け Advanced Malware Protection（AMP）8000 シリーズ アプライアンス
- FirePOWER 7000 シリーズ アプライアンス
- FirePOWER 8000 シリーズ アプライアンス
- サービス統合型ルータ（ISR）向け FirePOWER Threat Defense
- Blue Coat Xシリーズ向け次世代侵入防御システム(NGIPS)
- Sourcefire 3D システム アプライアンス
- VMware 向け仮想次世代侵入防御システム（NGIPSv）

Cisco FirePOWER システム ソフトウェアで何らかのファイル アクション ポリシーが設定されているかを確認するには、管理者は FirePOWER システムのダッシュボードで次の操作を実行します。

1. Policies > Access Control > Malware and Fileの順に選択します。システムに設定されたファイル アクション ポリシーのリストがダッシュボードに表示されます。
2. ポリシーの横にあるレポートアイコンをクリックして、ポリシーに現在保存されている設定の詳細を表示します。

各ファイルアクションポリシーは、特定の基準を満たすファイルの処理方法を定義する一連のルールとアクションを指定します。1つ以上のポリシーで Block Files、 Block Malware、または Detect Filesアクションが指定されている場合、システムに脆弱性が存在します。

この脆弱性は、ソースコードが —enable-file-inspect設定フラグを使用してコンパイルされている場合にも、オープンソースのSnortプロジェクトに影響を与えます。詳細については、Snort の Web サイトを参照してください。

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。

シスコは、この脆弱性が以下のシスコ製品には影響を与えないことを確認しました。

- 適応型セキュリティ アプライアンス（ASA）ソフトウェア
- FirePOWER 4100 シリーズ セキュリティ アプライアンス
- FirePOWER 9300 シリーズ セキュリティ アプライアンス
- Firepower Management Center
- 侵入防御システム（IPS）ソフトウェア
- サービス統合型ルータ（ISR）向け Snort IPS

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

シスコはこのアドバイザリに記載された脆弱性に対処する無償のソフトウェアアップデートをリリースしています。お客様がインストールしたりサポートを受けたりできるのは、ライセンスをご購入いただいたソフトウェア バージョンとフィーチャ セットに対してのみとなります。そのようなソフトウェアアップグレードをインストール、ダウンロード、アクセスまたはその他の方法で使用した場合、お客様は以下のリンクに記載されたシスコのソフトウェアライセンスの条項に従うことに同意したことになります。
http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html

また、お客様がソフトウェアをダウンロードできるのは、ソフトウェアの有効なライセンスをシスコから直接、あるいはシスコ認定リセラーやパートナーから取得している場合に限ります。通常、これは以前購入したソフトウェアのメンテナンス アップグレードです。無償のセキュリティ ソフトウェア アップデートによって、お客様に新しいソフトウェア ライセンス、追加ソフトウェア フィーチャ セット、またはメジャー リビジョン アップグレードに対する権限が付与されることはありません。

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。

サービス契約をご利用でないお客様

シスコから直接購入したがシスコのサービス契約をご利用いただいていない場合、また、サードパーティ ベンダーから購入したが修正済みソフトウェアを購入先から入手できない場合は、Cisco Technical Assistance Center（TAC）に連絡してアップグレードを入手してください。
http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html.

無償アップグレードの対象製品であることを証明していただくために、製品のシリアル番号と、本アドバイザリの URL をご用意ください。

修正済みリリース

この脆弱性は、Cisco Firepowerシステムソフトウェアの次のリリースで対処されています。

- 5.4.0.7 以降
- 5.4.1.6 以降
- 6.0.1 以降

Cisco Firepower Management Centerのソフトウェアアップデート機能を使用して、適切な修正済みリリースをインストールする必要があります。

この脆弱性は、Snortバージョン2.9.8.2以降でも対処されています。Snortユーザは、 Snort Webサイトから更新を取得できます。

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。

出典

この脆弱性は、Check Point Security TeamのDikla Barda、Liad Mizrachi、およびOded Vanunu氏によって発見され、シスコに報告されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160330-fp

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	初回公開リリース	—	Final	2016年3月30日

利用規約

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。