Cisco IronPortアプライアンスのSophosアンチウイルスの脆弱性

アドバイザリーID : cisco-sa-20121108-sophos
初公開日 : 2012-11-09 03:00
最終更新日 : 2012-11-13 23:16
バージョン 1.3 : Final
CVSSスコア : 9.7
回避策 : No Workarounds available
Cisco バグ ID : CSCud10546 CSCud10556

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 IronPort Email Security Appliances(ESA)およびCisco IronPort Web Security Appliances(WSA)には、複数の脆弱性を含むSophos Anti-Virusのバージョンが含まれており、認証されていないリモートの攻撃者がシステムを制御したり、権限を昇格したり、サービス妨害(DoS)状態を引き起こしたりする可能性があります。攻撃者は、Sophosアンチウイルスを実行しているアプライアンスに不正なファイルを送信することで、これらの脆弱性を不正利用する可能性があります。不正なファイルにより、Sophosウイルス対策エンジンが予期せぬ動作をする可能性があります。

2012年11月13日、シスコはこのドキュメントで説明されている脆弱性を修正するCisco IronPort ESAおよびWSAアップデートサーバに対してSophosエンジンの認定とプロビジョニングを行いました。

Sophosエンジンに対する今後のアップデートは、Cisco IronPort ESAおよびWSAアップデートサーバが使用可能になった時点で認定され、プロビジョニングされます。

このアドバイザリは、次のリンクより確認できます。
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20121108-sophos

シスコでは、シスコのお客様に影響を与えるアクティブな不正利用は確認していません。

該当製品

脆弱性のある製品

次のCisco IronPortアプライアンスがSophosソフトウェアを使用するように設定されている場合、この脆弱性の影響を受けます。

- Sophosエンジン3.2.07.352_4.80以前を実行するCisco IronPort Eメールセキュリティアプライアンス（Cシリーズおよびxシリーズ）
- Sophosエンジン3.2.07.352_4.80以前を実行しているCisco IronPort Webセキュリティアプライアンス（Sシリーズ）

お客様は、コマンドラインインターフェイス(CLI)またはWebグラフィカルユーザインターフェイス(GUI)を使用して、Sophosのソフトウェアとバージョンを確認できます。

Cisco IronPort WSA CLIで、versionコマンドを使用します。GUIでは、Security Services > Web Reputation and Anti-Malwareの順に選択します。

Cisco IronPort ESA CLIで、antivirusstatus sophosコマンドを使用します。GUIでは、Security Services > Anti-Virus > Sophosの順に選択します。

脆弱性を含んでいないことが確認された製品

Cisco IronPortセキュリティマネージメントアプライアンス（Mシリーズ）は、これらの脆弱性の影響を受けません。

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。

詳細

Cisco IronPort ESAは、スパム対策、ウイルス対策、および暗号化テクノロジーを組み合わせたEメール管理と保護を提供します。Cisco IronPort WSAは、高度なマルウェア防御、アプリケーションの可視性と制御、アクセプタブルユースポリシー(AUP)の制御、レポート、およびセキュアなモビリティを1つのプラットフォームで提供するセキュアなWebゲートウェイです。

Cisco IronPort ESAおよびWSAは、一般的なウイルス対策プログラムの1つを使用するように設定できます。Sophos Engine 3.2.07.352_4.80以前を実行しているCisco IronPortアプライアンスのみが、Sophosナレッジベースの記事 http://www.sophos.com/en-us/support/knowledgebase/118424.aspxで公開されている次の脆弱性の影響を受けます。

次の脆弱性は、Cisco IronPort ESAおよびWSA製品に現在インストールされているSophosエンジンに影響を与えます。

- Visual Basic 6コントロールを解析する整数オーバーフロー
- Internet Explorerの保護モードはSophosによって事実上無効にされています
- Microsoft CABパーサのメモリ破損の脆弱性
- RAR仮想マシン標準はメモリ破損をフィルタします
- PDFファイルを復号化するスタックバッファオーバーフロー

次の脆弱性は、現在Cisco IronPort ESAおよびWSA製品にインストールされているSophosエンジンには影響しません。

- sophos_detoured_x64.dll:ASLRバイパス
- ユニバーサルXSS
- ネットワーク更新サービスによる権限昇格

Sophosエンジンバージョン3.2.07.363_4.83は、2012年11月13日（火）にCisco IronPort ESAおよびWSAアップデートサーバで認定およびプロビジョニングされ、このドキュメントで説明されている脆弱性が修正されています。

これらの脆弱性は、Cisco IronPort Email Security Applianceについては CSCud10556(登録ユーザ専用)に、Cisco IronPort Web Security Applianceについては CSCud10546(登録ユーザ専用)に記載されています。

回避策

この脆弱性に対する回避策はありません。 Sophosエンジンバージョン3.207.363_4.83にアップデートすることをお勧めします。

修正済みソフトウェア

Sophosエンジンバージョン3.2.07.363_4.83は、2012年11月13日にCisco IronPort ESAおよびWSAアップデートサーバで認定およびプロビジョニングされ、このアドバイザリで説明されている脆弱性が修正されています。

推奨事項

$propertyAndFields.get("recommendations")

不正利用事例と公式発表

Cisco IronPortアプライアンスに影響を与えるSophosアンチウイルスの脆弱性は、2012年11月5日にTavis Ormandy氏によって公開されました。Sophosアドバイザリは次のリンクに掲載されています。

http://www.sophos.com/en-us/support/knowledgebase/118424.aspx

シスコでは、シスコのお客様に影響を与えるアクティブな不正利用は確認していません。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20121108-sophos

改訂履歴

リビジョン 1.3	2012年11月13日	修正済みソフトウェアを通知するように更新。
リビジョン 1.2	2012年11月12日	予想される修正の提供状況を追加。
リビジョン 1.1	2012年11月9日	追加のCLI/GUIコマンドを追加。
リビジョン 1.0	2012年11月9日	初回公開リリース

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。