Cisco ESAおよびWSA AMP ClamAVのDoS脆弱性

Medium

アドバイザリーID : cisco-sa-20160531-wsa-esa
初公開日 : 2016-05-31 10:30
バージョン 1.0 : Final
CVSSスコア : 5.0
回避策 : No workarounds available
Cisco バグ ID : CSCuw60503 CSCuv78533

CVE-2016-1405

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 Eメールセキュリティアプライアンス(ESA)およびCisco Webセキュリティアプライアンス(WSA)用のCisco Advance Malware Protection(AMP)で使用されるClam AntiVirus(ClamAV)ソフトウェアの脆弱性により、認証されていないリモートの攻撃者がAMPプロセスを再起動させる可能性があります。

この脆弱性は、 libclamavライブラリによる入力ファイルの不適切な解析に起因します。攻撃者は、該当システムのAMP ClamAVライブラリからのスキャンをトリガーする巧妙に細工されたドキュメントを送信することで、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AMPプロセスを再起動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-20160531-wsa-esa

該当製品

脆弱性のある製品

この脆弱性は、該当ソフトウェアリリースを実行している次のシスコ製品に影響を与えます。

- Clam AntiVirus(ClamAV)

- E メール セキュリティ アプライアンス（ESA）
- Web セキュリティ アプライアンス（WSA）

脆弱性を含んでいないことが確認された製品

この脆弱性は、次のシスコ製品には影響しません。

- ネットワーク、7000および8000シリーズアプライアンス向けAdvanced Malware Protection
- AnyConnect セキュア モビリティ クライアント
- ASA 5500-X with FirePOWER Services シリーズ
- クラウド Web セキュリティ
- コンテンツセキュリティ管理アプライアンス(SMA)
- FireAMP
- Firepower 4100 シリーズ
- 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
- Firepower 9300 シリーズ

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

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。

この脆弱性は、次のCisco AsyncOSソフトウェアリリースで対処されています。

- Cisco ESAでは9.7.0-125以降
- Cisco WSAでは9.0.1-135以降
- Cisco WSAでは9.1.1-041以降

この脆弱性は、ClamAVリリース0.99以降でも対処されています。

推奨事項

$propertyAndFields.get("recommendations")

不正利用事例と公式発表

Cisco 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、サポートケースの解決中に発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160531-wsa-esa

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 月 5 月 31 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。