Multiple Vulnerabilities in Cisco Email Security Appliance

Advisory ID: cisco-sa-20130626-esa

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130626-esa

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。

Revision 1.0

For Public Release 2013 June 26 16:00 UTC (GMT)

目次

要約

Cisco E メール セキュリティ アプライアンス (ESA) 用の Cisco IronPort AsyncOS ソフトウェアは、次の脆弱性の影響を受けます。

- Web フレームワークの認証されたコマンド インジェクションにおける脆弱性
- IronPort スパム検疫における DoS 脆弱性
- 管理 GUI における DoS 脆弱性

Web フレームワークの認証されたコマンド インジェクションにおける脆弱性の不正利用に成功した場合、認証された攻撃者がリモートから権限を昇格して、基盤のオペレーティング システムで任意のコマンドを実行する可能性があります。
2 つの DoS 脆弱性のいずれかの不正利用に成功した場合、複数の重要なプロセスが応答しなくなり、影響を受けるシステムが不安定になる可能性があります。

シスコはこれらの脆弱性に対応するための無償ソフトウェア アップデートを提供しています。これらの脆弱性に対しては回避策があります。このアドバイザリは、次のリンクで確認できます。

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130626-esa

該当製品

脆弱性が認められる製品

脆弱性のあるバージョンの Cisco IronPort AsyncOS ソフトウェアを実行している Cisco E メール セキュリティ アプライアンス (ESA) のすべてのモデルは、このアドバイザリに記載された 1 つ以上の脆弱性の影響を受けます。

このアドバイザリに記載された脆弱性の一部は、Cisco Web セキュリティと Cisco コンテンツ セキュリティ マネージメント アプライアンス (SMA) 用の Cisco IronPort AsyncOS ソフトウェアに影響します。
Cisco Web セキュリティ アプライアンス (WSA) に影響する脆弱性の詳細については、Cisco Security Advisory『*Cisco Web セキュリティ アプライアンス (WSA) における複数の脆弱性*』（ http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130626-wsa ）を、Cisco コンテンツ セキュリティ マネージメント アプライアンス (SMA) に影響する脆弱性の詳細については、Cisco Security Advisory『*Cisco コンテンツ セキュリティマネージメント アプライアンス (SMA) における複数の脆弱性*』（ http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130626-sma ）を確認してください。

実行中のソフトウェア バージョンの確認

脆弱性のあるバージョンの Cisco IronPort AsyncOS ソフトウェアがアプライアンスで実行されているかどうかを知るには、**version** コマンドを発行します。次の例は Cisco IronPort AsyncOS ソフトウェア バージョン 7.6.2-201 を実行しているデバイスを示しています。

```
ciscoesa> version
Current Version
===============
Product: Cisco IronPort X1070 Messaging Gateway(tm) Appliance
Model: X1070
Version: 7.6.2-201
[...]
```

脆弱性が認められない製品

Cisco コンテンツ セキュリティ マネージメント (SMA) と Cisco Web セキュリティ アプライアンス (WSA) 以外には、脆弱性の影響を受けるその他のシスコ製品は現在確認されていません。

詳細

Cisco E メール セキュリティ アプライアンス (ESA) では、アンチスパム、アンチウイルス、および暗号化技術を組み合わせて、E メールを管理して保護することができます。

Web フレームワークの認証されたコマンド インジェクションにおける脆弱性

Web フレームワーク コード内の脆弱性が利用されると、認証された攻撃者がリモートから権限を昇格して基盤のオペレーティング システムで任意のコマンドを実行する可能性があります。

この脆弱性は、デバイスの基盤のコマンドライン インターフェイスを利用してアクションを実行

するためのユーザの入力を適切にサニタイズできないことに起因します。権限のない認証された攻撃者は、影響を受けるシステムに細工された URL を送信することか、有効なユーザに悪意のある URL をクリックさせることで、この脆弱性を不正利用する可能性があります。不正利用に成功した場合、十分な知識を持つ攻撃者が影響を受けるデバイスを完全に制御できるようになる可能性があります。

この脆弱性は、影響を受けるシステムの管理 IP アドレスに IPv4 トラフィックと IPv6 トラフィックを送信することで引き起こされます。
この脆弱性はデフォルトの管理ポートである TCP ポート 80 または 443 で不正利用される可能性があります。

注：デフォルトの管理ポートはシステムで再設定できます。

この脆弱性は、Cisco Bug ID CSCzv44633（ 登録ユーザ専用 ）として文書化され、Common Vulnerabilities and Exposures（CVE）ID として CVE-2013-3384 が割り当てられています。

IronPort スパム検疫における DoS 脆弱性

ISQ（IronPort スパム検疫）機能に存在する脆弱性が利用されると、認証されていない攻撃者がリモートから複数の重要なプロセスを応答不能にして、DoS の状態にする可能性があります。

この脆弱性は、大量に送信された TCP 接続リクエストが適切に処理されないことに起因します。攻撃者は、影響を受けるシステムの ISQ 対応インターフェイスで開かれている ISQ サービス ポートに TCP リクエストを連続して送信することで、この脆弱性を不正利用する可能性があります。この脆弱性を不正利用するには、完全な TCP 3 ウェイ ハンドシェイクが必要です。不正利用に成功した場合、攻撃者がクラッシュや ISQ サービスの応答不能を発生させて、DoS の状態にする可能性があります。すべての機能を復元するには、影響を受けたシステムのハード リブートが必要です。
この脆弱性は、影響を受けるシステムの ISQ 対応インターフェイスに IPv4 トラフィックと IPv6 トラフィックを送信することで引き起こされます。
この脆弱性は、デフォルトの ISQ ポートである TCP 82 または 83 で不正利用される可能性があります。**注**：デフォルトの ISQ ポートはサーバで再設定できます。この脆弱性は、Cisco Bug ID CSCzv25573（ 登録ユーザ専用 ）として文書化され、CVE ID として CVE-2013-3386 が割り当てられています。

管理 GUI における DoS 脆弱性

Web フレームワーク コードのグラフィカル ユーザ インターフェイス（GUI）機能に存在する脆弱性が利用されると、認証されていない攻撃者がリモートから複数のプロセスを応答不能にして、DoS の状態にする可能性があります。

この脆弱性は、HTTP 接続と HTTPS 接続の操作、処理、および終了が適切に行われないことに起因します。攻撃者は、攻撃対象システムの管理がイネーブルなインターフェイスに HTTP または HTTPS の複数のリクエス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。この脆弱性を不正利用するには、完全な TCP 3 ウェイ ハンドシェイクが必要です。不正利用されると、攻撃者は GUI からの管理アクセスを妨げて、他の重要なプロセスを応答不能にして、DoS の状態にする可能性があります。すべての機能を復元するには、影響を受けたシステムのハード リブートが必要です。

この脆弱性は、影響を受けるシステムの管理 IP アドレスに IPv4 トラフィックと IPv6 トラフィックを送信することで引き起こされます。この脆弱性はデフォルトの管理ポートである TCP ポート 80 または 443 で不正利用される可能性があります。 **注**：デフォルトの管理ポートはシステムで再設定できます。この脆弱性は、Cisco Bug ID CSCzv63329（ 登録ユーザ専用 ）として文書化

され、CVE ID として CVE-2013-3385 が割り当てられています。

脆弱性スコア詳細

シスコはこのアドバイザリでの脆弱性に対して Common Vulnerability Scoring System（CVSS）に基づいたスコアを提供しています。本セキュリティ アドバイザリでの CVSS スコアは、CVSS バージョン 2.0 に基づいています。

CVSS は、脆弱性の重要度を示唆するもので、緊急性および対応の優先度を決定する組織の手助けとなる標準ベースの評価法です。

シスコでは、基本評価スコア（Base Score）および現状評価スコア（Temporal Score）を提供しています。お客様はこれらを用いて環境評価スコア（Environmental Score）を算出し、自身のネットワークにおける脆弱性の影響度を知ることができます。

シスコは次のリンクで CVSS に関する追加情報を提供しています。

http://www.cisco.com/web/about/security/intelligence/cvss-qandas.html

またシスコでは、各ネットワークにおける環境影響度を算出する CVSS 計算ツールを次のリンクで提供しています。

http://tools.cisco.com/security/center/cvssCalculator.x/

CSCzv44633 - Web Framework Authenticated Command Injection Vulnerability Calculate the environmental score of					
CVSS Base Score - **9.0**					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	Single	Complete	Complete	Complete
CVSS Temporal Score - **7.4**					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

CSCzv25573 - IronPort Spam Quarantine Denial of Service Vulnerability Calculate the environmental score of					
CVSS Base Score - **7.8**					
Access	Access Comple	Authentication	Confidentiality	Integrity	Availability

Vector	xity		Impact	Impact	Impact
Network	Low	None	None	None	Complete
CVSS Temporal Score - **6.4**					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

CSCzv63329 - Management GUI Denial of Service Vulnerability Calculate the environmental score of					
CVSS Base Score - **7.8**					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	None	None	Complete
CVSS Temporal Score - **6.4**					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

影響

Web フレームワークの認証されたコマンド インジェクションにおける脆弱性の不正利用に成功した場合、認証された攻撃者がリモートから権限を昇格して、基盤のオペレーティング システムで任意のコマンドを実行する可能性があります。
2 つの DoS 脆弱性のいずれかの不正利用に成功した場合、複数の重要なプロセスが応答しなくなり、影響を受けるシステムが不安定になる可能性があります。

ソフトウェア バージョンおよび修正

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, Responses, and Notices アーカイブや、後続のアドバイザリを参照して、起こりうる障害を判断し、それに対応できるアップグレード 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、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。

次の表に、Web フレームワークの認証されたコマンド インジェクションにおける脆弱性への修正が含まれた最初の修正済みリリースのリストを記載します。

Major Release	First Fixed In
7.1 and prior	7.1.5-104
7.3	7.3.2-026
7.5	7.5.2-203
7.6	7.6.3-019
8.0	Not Affected

次の表に、 IronPort スパム検疫における DoS 脆弱性への修正が含まれた最初の修正済みリリースのリストを記載します。

Major Release	First Fixed In
7.1 and prior	7.1.5-106
7.3	Not available; migrate to 8.0.0-671 or later
7.5	Not available; migrate to 7.6.3-019 or later
7.6	7.6.3-019
8.0	Not Affected

次の表に、 管理 GUI における DoS 脆弱性への修正が含まれた最初の修正済みリリースのリストを記載します。

Major Release	First Fix In
7.1 and prior	7.1.5-106
7.3	Not available, migrate to 8.0.0-671 or later
7.5	Not available, migrate to 7.6.3-019 or later
7.6	7.6.3-019
8.0	Not Affected

次の表に、このセキュリティ アドバイザリで説明のあるすべての脆弱性への修正が含まれた推奨リリースを記載します。

Major Release	Recommended
7.1 and prior	7.1.5-106 or later
7.3	8.0.0-671 or later
7.5	7.6.3-019 or later
7.6	7.6.3-019 or later

回避策

Web フレームワークの認証されたコマンド インジェクションの脆弱性と管理 GUI における DoS 脆弱性は、影響を受けるシステムの GUI への管理アクセスを無効にすることで回避できます。 **interfaceconfig** コマンドを使用して GUI からのアプライアンス管理を無効にできます。あるいは、GUI の [Network] -> [IP interfaces] -> [Edit] で管理インターフェイスのプロパティを編集し、Appliance Management セクションの設定変更を行うことで、管理を無効にできます。

注：GUI へのアクセスが無効化されているときは、SSH とコマンドライン インターフェイスを使用して、影響を受けるシステムを管理できます。ただし、一部のコマンドと機能はコマンドラ

イン インターフェイスから使用できない場合があります。

管理インターフェイスにアクセスできる IP アドレスを限定して、攻撃箇所も制限できます。これを行うには、 **adminaccessconfig** コマンドを使用し、メニューの [IPACCESS] を選択します。

プラットフォームとソフトウェア リリースで使用可能な場合は、クロスサイト リクエスト フォージェリの防御策も実装する必要があります。この実装により、Web フレームワークの認証されたコマンド インジェクションの脆弱性の攻撃箇所を制限できます。ただし、完全になくすことはできません。

IronPort スパム検疫における DoS 脆弱性は、ISQ サービスへのエンドユーザ アクセスを無効にすることで回避できます。 **interfaceconfig** コマンドを使用してこのアクセスを無効にできます。あるいは、GUI の [Monitor] -> [Quarantines] -> [Edit] でスパム検疫の設定を編集し、[Enable End-User Quarantine Access] チェックボックスをオフにすることで、アクセスを無効にできます。

注：エンドユーザ アクセスが無効なときは、ユーザはセーフ リストとブロック リストを管理できません。

回避策の詳細は、このアドバイザリの付属ドキュメントである『Applied Mitigation Bulletin（AMB）』にて参照できます。
http://tools.cisco.com/security/center/viewAMBAlert.x?alertId=29452

修正済みソフトウェアの入手

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 アップデートを提供しています。ソフトウェアの導入を行う前に、お客様のメンテナンス プロバイダーにご相談いただくか、ソフトウェアのフィーチャ セットの互換性およびお客様のネットワーク環境の特有の問題をご確認ください。

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、ご購入いただいたフィーチャ 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 http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html に記載の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。

サービス契約をご利用のお客様

サービス契約をご利用のお客様は、通常のアップデート チャネルからアップグレード ソフトウェアを入手してください。ほとんどのお客様は、Cisco.com の Software Navigator からアップグレード ソフトウェアを入手できます。http://www.cisco.com/cisco/software/navigator.html

サードパーティのサポート会社をご利用のお客様

シスコ パートナー、正規販売代理店、サービス プロバイダーなど、サードパーティのサポート会社と以前に契約していたか、または現在契約しており、その会社からシスコ製品の提供または保守を受けているお客様は、該当するサポート会社に連絡し、正しい処置についてのサポートを受けてください。

回避策や修正の効果は、使用している製品、ネットワーク トポロジー、トラフィックの性質や組織の目的などに関するお客様の状況によって異なります。影響を受ける製品やリリースは多種多様であるため、回避策を実施する前に、対象ネットワークで適用する回避策または修正が最適であることを、お客様のサービス プロバイダーやサポート会社にご確認ください。

サービス契約をご利用でないお客様

シスコから製品を直接購入したもののシスコのサービス契約をご利用いただいていない場合、または、サードパーティ ベンダーから購入したものの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 ソフトウェアを入手してください。

- +1 800 553 2447（北米からの無料通話）
- +1 408 526 7209（北米以外からの有料通話）
- E メール：tac@cisco.com

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。サービス契約をご利用でないお客様は TAC に無償アップグレードをリクエストしてください。

多言語による各地の電話番号、説明、E メール アドレスなどの TAC の連絡先情報については、Cisco Worldwide Contact を参照してください。
http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html

不正利用事例と公式発表

Cisco Product Security Incident Response Team（PSIRT）では、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とその公表は確認しておりません。

これらの脆弱性は、影響を受ける製品の社内セキュリティ調査で特定されました。

この通知のステータス：FINAL

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を示唆するものでもありません。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。またシスコはいつでも本ドキュメントの変更や更新を実施する権利を有します。

後述する情報配信の URL を省略し、本アドバイザリの記述内容に関して単独の転載や意訳を実施した場合には、事実誤認ないし重要な情報の欠落を含む統制不可能な情報の伝搬が行われる可能性があります。

情報配信

このアドバイザリは次のリンクにある Cisco Security Intelligence Operations に掲載されます。

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130626-esa

また、このアドバイザリのテキスト版が Cisco PSIRT PGP キーによるクリア署名つきで次の E メールで配信されています。

- cust-security-announce@cisco.com
- first-bulletins@lists.first.org

- bugtraq@securityfocus.com
- vulnwatch@vulnwatch.org
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- full-disclosure@lists.grok.org.uk

本アドバイザリに関する今後の更新は Cisco.com に掲載されますが、メーリング リストで配信されるとは限りません。更新内容については、本アドバイザリの URL でご確認ください。

更新履歴

Revision 1.0	2013-June-26	Initial public release

シスコ セキュリティ手順

シスコ製品におけるセキュリティの脆弱性の報告、セキュリティ事故に関するサポート、およびシスコからセキュリティ情報を入手するための登録方法の詳細については、Cisco.com の http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html を参照してください。この Web ページには、シスコのセキュリティ アドバイザリに関してメディアが問い合わせる際の指示が掲載されています。シスコ セキュリティ アドバイザリについては、すべて http://www.cisco.com/go/psirt/ で確認できます。