Cisco Security Advisory: Cisco AsyncOS Software Code Execution Vulnerability

Advisory ID：cisco-sa-20140319-asyncos

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140319-asyncos

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 2014 March 19 16:00 UTC (GMT)

目次

要約

E メール セキュリティ アプライアンス（ESA）および Cisco コンテンツ セキュリティ管理アプライアンス（SMA）用の Cisco AsyncOS ソフトウェアには、リモートの認証された攻撃者が *root* ユーザの権限を使用して任意のコードを実行できる可能性のある脆弱性が存在します。

シスコはこの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ました。これらの脆弱性に対しては回避策がありません。このアドバイザリは、次のリンクで確認できます。
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140319-asyncos

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 ソフトウェアまたは Cisco AsyncOS ソフトウェアを実行している Cisco ESA および Cisco SMA のすべてのモデルは、このセキュリティ ア

ドバイザリに記載された脆弱性の影響を受けます。

攻撃者がこの脆弱性を不正利用するには、該当するシステム上で FTP サービスと セーフリスト/ブロックリスト（SLBL）サービスを有効にする、またはこれらのサービスがすでに有効になっていることを確認して利用する、あるいはこれらのサービスを一時的に有効にするようシステム管理者を誘導する必要があります。

注：これらの 2 つのサービスを同時に有効にしなくても攻撃は成功します。

FTP サービスが新しい接続をアクティブにリスニングしているかどうかを調べるには、Cisco ESA または Cisco SMA のコマンドライン インターフェイス（CLI）から **netstat** コマンドを使用して、TCP ポート 21 が LISTEN 状態であることを確認します。

次の例は、FTP サービスがアクティブ（LISTEN 状態）になっている Cisco ESA を示しています。

```
ciscoesa> netstat

Choose the information you want to display:
1. List of active sockets.
2. State of network interfaces.
3. Contents of routing tables.
4. Size of the listen queues.
5. Packet traffic information.
[1]>

1. IPv4 only.
2. IPv6 only.
[1]>

Show network addresses as numbers? [N]> y

Avoid truncating addresses? [N]>

Active Internet connections (including servers)
Proto Recv-Q Send-Q Local Address Foreign Address (state)
tcp4 0 0 172.18.254.17.443 *.* LISTEN
tcp4 0 0 172.18.254.17.80 *.* LISTEN
tcp4 0 0 172.18.254.17.25 *.* LISTEN
tcp4       0      0 172.18.254.17.21       *.*                    LISTEN
```

注：TCP ポート 21 は FTP サービスのデフォルト ポートです。ただし、FTP サービスで使用するポートは、FTP サービスをアクティブにするときに設定できます。お客様は開いているすべてのポートを調べ、別のポートで FTP サービスが有効になっているかどうかを確認する必要があります。
Cisco ESA および Cisco SMA 用の Cisco AsyncOS ソフトウェアのバージョンによっては、FTP サービスがデフォルトで有効になる場合があります。

SLBL サービスが有効になっているかどうかを調べるには、 **slblconfig** コマンドを使用します。次の例は、SLBL サービスが有効になっている Cisco ESA を示しています。

```
ciscoesa> slblconfig
End-User Safelist/Blocklist: Enabled
[...]
```

注：SLBL サービスはデフォルトでは有効になりません。

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 AsyncOS ソフトウェアが Cisco ESA で実行されているかどうかを調べるには、**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> slblconfig
End-User Safelist/Blocklist: Enabled
[...]
```

脆弱性のあるバージョンの Cisco AsyncOS ソフトウェアが Cisco SMA で実行されているかどうかを調べるには、**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 7.9.1-039 を実行しているデバイスを示しています。

```
ciscoesa> slblconfig
End-User Safelist/Blocklist: Enabled
[...]
```

脆弱性が認められない製品

Cisco Web セキュリティ アプライアンス（WSA）用 Cisco AsyncOS ソフトウェアは、この脆弱性の影響を受けません。

他のシスコ製品において、この脆弱性の影響を受けるもの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。

Cisco コンテンツ セキュリティ管理アプライアンス（SMA）は、ポリシーとランタイム データを単一の管理インターフェイスに統合し、Cisco E メール セキュリティ アプライアンス（ESA）および Web セキュリティ アプライアンス（WSA）のレポーティングと監査のすべてに、一元化されたプラットフォームで対応します。

Cisco E メール セキュリティ アプライアンスおよび Cisco コンテンツ セキュリティ管理アプライアンス用 Cisco AsyncOS ソフトウェアのエンド ユーザ セーフリスト/ブロックリスト（SLBL）機能の脆弱性により、認証されたリモートの攻撃者によって該当するシステム上で任意のコードが実行される可能性があります。

この脆弱性は、SLBL データベース ファイルの検証が不十分であることに起因します。有効な SLBL データベース ファイルを、改ざんされたファイルに置き換えると、この脆弱性を不正利用できます。改ざんされたファイルにはシェル コードが含まれていることがあり、特定のイベントの発生時（たとえば、新しい E メールの受信時に SLBL チェックが実行される場合）に、該当するシステム上でそのシェル コードが実行されます。攻撃者がこの脆弱性を不正利用するには、FTP および SLBL サービスを少なくとも一時的に有効にし、改ざんされた SLBL データベース ファイルを FTP 経由でアップロードするための資格情報を入手する必要があります。

この不正利用により、攻撃者は *root* ユーザの権限を使用して、該当するシステム上で任意のコードを実行できる場合があります。

この脆弱性は、Cisco ESA については Cisco Bug ID CSCug79377（ 登録ユーザ専用）、および Cisco コンテンツ SMA については CSCug80118（ 登録ユーザ専用）によって文書化されていま

す。この脆弱性に対して Common Vulnerabilities and Exposures（CVE）ID CVE-2014-2119 が割り当てられています。

脆弱性スコア詳細

シスコは本アドバイザリでの脆弱性に対し、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/

CSCug79377 and CSCug80118 - Cisco AsyncOS Software SLBL Code Execution Vulnerability Calculate the environmental score of					
CVSS Base Score - **8.5**					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Medium	Single	Complete	Complete	Complete
CVSS Temporal Score - **7.0**					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

影響

この脆弱性の不正利用により、*root* ユーザの権限を使用して、該当するシステム上で任意のコードが実行され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、本アドバイザリに記載される脆弱性を修正する最初のリリースに関する情報を、Cisco ESA 用 Cisco AsyncOS ソフトウェアのメジャー リリース バージョン別に示します。

Major Release	First Fixed In
7.1 and prior	Migrate to 7.6.3-023 or later
7.3	Migrate to 8.0.1-023 or later
7.5	Migrate to 7.6.3-023 or later
7.6	7.6.3-023 or later
7.8	Migrate to 8.0.1-023 or later
8.0	8.0.1-023 or later
8.5	Not affected

次の表に、本アドバイザリに記載される脆弱性を修正する最初のリリースに関する情報を、Cisco SMA 用 Cisco AsyncOS ソフトウェアのメジャー リリース バージョン別に示します。

Major Release	First Fixed In
7.2 and prior	Migrate to 7.9.1-110 or later
7.7	Migrate to 7.9.1-110 or later
7.8	Migrate to 7.9.1-110 or later
7.9	7.9.1-110 or later
8.0	Migrate to 8.1.1-013 or later
8.1	8.1.1-013 or later
8.2	Not Affected
8.3	Not Affected

回避策

この脆弱性を軽減する回避策はありません。FTP サービスを無効にすると、SLBL データベース ファイルが悪意のあるファイルに置き換えられるのを回避できるため、この脆弱性の影響を軽減できます。

GUI から FTP サービスを無効にするには、[**Network**] > [**IP Interfaces**] に移動します。インターフェイスごとにインターフェイス名をクリックし、[Edit] ウィンドウのサービス領域にある [FTP] チェック ボックスをオフにします。

また、CLI を使用することもできます。CLI から FTP サービスを無効にするには、**interfaceconfig** コマンドを使用し、[**EDIT**] を選択してインターフェイスの設定を編集します。プ

ロンプトが表示されたら、*N* と入力して FTP サービスを無効にし、commit コマンドを使用して変更を確定します。次の例は、Cisco ESA で FTP サービスを無効にする方法を示しています。

```
ciscoesa> interfaceconfig


Currently configured interfaces:
1. Management (192.168.42.42/24 on Management: ciscoesa)

Choose the operation you want to perform:
- NEW - Create a new interface.
- EDIT - Modify an interface.
- GROUPS - Define interface groups.
- DELETE - Remove an interface.
[]> edit

Enter the number of the interface you wish to edit.
[]> 1

IP interface name (Ex: "InternalNet"):
[Management]>

Would you like to configure an IPv4 address for this interface (y/n)? [Y]>

IPv4 Address (Ex: 192.168.1.2 ):
[192.168.42.42]>

Netmask (Ex: "24", "255.255.255.0" or "0xffffff00"):
[24]>

Would you like to configure an IPv6 address for this interface (y/n)? [N]>

Ethernet interface:
1. Data 1
2. Data 2
3. Management
[3]>

Hostname:
[ciscoesa]>

Do you want to enable Telnet on this interface? [N]>

Do you want to enable SSH on this interface? [Y]>

Which port do you want to use for SSH?
[22]>

Do you want to enable FTP on this interface? [Y]>  (Set option to 'N') this
will disable the service once change has been committed.

Which port do you want to use for FTP?
[21]>

Do you want to enable Cluster Communication Service on this interface? [N]>

Do you want to enable HTTP on this interface? [Y]>

Which port do you want to use for HTTP?
[80]>

Do you want to enable HTTPS on this interface? [Y]>
```

```
Which port do you want to use for HTTPS?
[443]>

Do you want to enable Spam Quarantine HTTP on this interface? [Y]>

Which port do you want to use for Spam Quarantine HTTP?
[82]>

Do you want to enable Spam Quarantine HTTPS on this interface? [Y]>

Which port do you want to use for Spam Quarantine HTTPS?
[83]>

Do you want to enable RSA Enterprise Manager Integration on this interface?
[N]>

The "Demo" certificate is currently configured. You may use "Demo", but
this will not be secure. To assure privacy, run "certconfig" first.

Both HTTP and HTTPS are enabled for this interface, should HTTP requests
redirect to the secure service? [Y]>

Both Spam Quarantine HTTP and Spam Quarantine HTTPS are enabled for this
interface, should Spam Quarantine HTTP requests redirect to the secure
service? [Y]>

Do you want Management as the default interface for your Spam Quarantine?
[N]>


Currently configured interfaces:
1. Management (192.168.42.42/24 on Management: ironport.example.com)

Choose the operation you want to perform:
- NEW - Create a new interface.
- EDIT - Modify an interface.
- GROUPS - Define interface groups.
- DELETE - Remove an interface.
[]>

ciscoese> commit

Please enter some comments describing your changes:
[]> disabled FTP
```

FTP サービスを無効にするだけでなく、SLBL サービスも無効にすると、悪意のある SLBL データベース ファイルのコンテンツの実行を回避できるため、この脆弱性の影響を軽減できます。

SLBL は GUI からのみ無効にできます。[**Monitor**] > [**Spam Quarantine**] に移動し、[End-User Safelist/Blocklist (Spam Quarantine)] 領域の [**Edit Setting**] ボタンをクリックします。[Edit] ウィンドウで、[**Enable End User Safelist/Blocklist Feature**] チェックボックスをオフにし、[**Submit**] をクリックします。

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を入手することができます。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。

さまざまな言語向けの各地の電話番号、説明、電子メール アドレスなどの、この他の TAC の連絡先情報については、シスコ ワールドワイドお問い合わせ先（http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html）を参照してください。

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。

この脆弱性はシスコ内部でのセキュリティ テストによって発見されました。

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-20140319-asyncos

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	2014-March-19	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/web/about/security/psirt/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。すべてのシスコ セキュリティ アドバイザリは、http://www.cisco.com/go/psirt/ で確認することができます。