Cisco Security Advisory: Cisco IronPort Appliances Telnet Remote Code Execution Vulnerability

Advisory ID: cisco-sa-20120126-ironport

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120126-ironport

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 1.3

Last Updated 2012 February 8 15:20 UTC (GMT)

For Public Release 2012 January 26 17:00 UTC (GMT)

目次

要約

Cisco IronPort E メール セキュリティ アプライアンス（ESA）および Cisco IronPort セキュリティ マネジメント アプライアンス（SMA）には、リモートの認証されていない攻撃者が権限昇格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。

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、次のリンク先で確認できます。
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120126-ironport

該当製品

脆弱性が存在する製品

この脆弱性の影響を受ける Cisco IronPort E メール セキュリティ アプライアンス（ESA）および Cisco IronPort セキュリティ マネジメント アプライアンス（SMA）は、次のとおりです。

バージョンが 7.6.0 より前の 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）
バージョンが 7.8.0 より前の Cisco IronPort セキュリティ マネジメント アプライアンス（M シリーズ）

脆弱性が存在しない製品

Cisco IronPort Web セキュリティ アプライアンス（S シリーズ）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 IronPort ESA では、アンチスパム、アンチウィルス、暗号化、デジタル著作権管理、およびアーカイブ技術を組み合わせて、電子メールを管理および保護することができます。Cisco IronPort SMA は、ポリシーおよびランタイム データを集中管理および統一するために設計された柔軟性の高い管理ツールであり、単一の管理インターフェイスを通じて複数の Cisco IronPort セキュリティ アプライアンスを管理することができます。

Cisco IronPort ESA および Cisco IronPort SMA は、改変版の FreeBSD カーネルである AsyncOS を実行します。

これらのデバイスは、FreeBSD の *telnetd* におけるリモート コード実行の脆弱性の影響を受けます。この脆弱性については Common Vulnerabilities and Exposures（CVE）の CVE ID CVE-2011-4862 に記載されています。この脆弱性によって、リモートの認証されていない攻撃者が権限昇格を使用して任意のコードを実行できる可能性があります。

この脆弱性は、Cisco IronPort Bug 83262 に文書化されています。

注：Cisco IronPort は、お客様には非公開の内部システムを使用してバグを追跡します。Cisco IronPort のバグ トラッキング ID は参照用としてのみ提供しています。

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。このセキュリティ 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導き出すことができます。

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、シスコは個々の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

CVE-2011-4862 - Telnetd encrypt_keyid vulnerability (Ironport #83262) Calculate the environmental score of CVE-2011-4862					
CVSS Base Score - **10.0**					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	Complete	Complete	Complete
CVSS Temporal Score - **9.0**					
Exploitability		Remediation Level		Report Confidence	
Functional		Workaround		Confirmed	

影響

この脆弱性の不正利用に成功した場合、リモートの認証されていない攻撃者が権限昇格を使用して任意のコードを実行でき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

このアドバイザリに記載された脆弱性に対する修正は、まだ全ての製品では完了していません。しかし、ほとんどのお客様でリスクを排除できる定義変更による回避策があります。 この脆弱性に対する回避策の情報は、アドバイザリの「回避策」セクションをご参照下さい。

Affected Product	Affected Versions	Fixed Versions
Cisco IronPort Email Security Appliance (C-Series and X-Series)	versions prior to 7.6.0	phoebe-7-2-2-106 phoebe-7-5-1-102 phoebe-7-7-0-206
Cisco IronPort Security Management Appliance (M-Series)	versions prior to 7.8.0	Not yet available **

Cisco IronPort Email Security Appliance (C-Series および X-Series) バージョン 7.6.0 はこの問題の修正が適用されてリリースされます。

** Cisco IronPort Security Management Appliance (M-Series) バージョン 7.8.0 および 7.9.0 はこ

の問題の修正が適用されてリリースされます。

アップグレードが可能になった際は、お客様は CLI または GUI によりシステム アップグレードを行うことができます。 CLI では *upgrade* コマンドを使用します。 GUI では **System Administration > System Upgrades** を選択します。 システムが適用可能なアップグレードを確認し、アップグレード バージョンを提供します。 IronPort アプライアンスがアップグレードを実行している間でもメールの処理は継続されます。 アップグレードには再起動が必要です。

回避策

デフォルトでは、Telnet が管理ポートに設定されています。Telnet サービスを無効にすることで、この脆弱性を緩和することができます。管理者はグラフィカル ユーザ インターフェイス（GUI）を使用するか、コマンドライン インターフェイス（CLI）で interfaceconfig コマンドを使用して、Telnet を無効にすることができます。セキュリティのベスト プラクティスとして、Telnet ではなくセキュア シェル（SSH）を使用してください。

GUI を介して Telnet を無効にするには、次の手順を実行します。

ステップ 1：**[Network] > [IP Interfaces]** > [interface_name] に移動します。
ステップ 2：**Telnet** サービスの横にあるボックスをオフにします。
ステップ 3：**[Submit]** ボタンをクリックして、変更を送信します。
ステップ 4：**[Commit Change]** ボタンをクリックして、これらの変更内容を反映します。

interfaceconfig コマンドを使用して、CLI から Telnet を無効にする場合は次のようにします。

```
mail3.example.com> interfaceconfig

Currently configured interfaces:
1. Data 1 (192.168.1.1/24 on Data1: mail3.example.com)
2. Data 2 (192.168.2.1/24 on Data2: mail3.example.com)
3. Management (192.168.42.42/24 on Management: mail3.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.

[]> edit
Enter the number of the interface you wish to edit.
[]> 3

<..output omitted>

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

注： interfaceconfig コマンドの詳細については、次のリンクをクリックして、『Cisco IronPort AsyncOS Daily Management Guide』の「*Other Tasks in the GUI*」セクションを参照してください。
http://www.cisco.com/en/US/docs/security/esa/esa7.5/ESA_7.5_Daily_Management_Guide.pdf

Cisco Applied Mitigation Bulletin（AMB）の『Identifying and Mitigating Exploitation of the Cisco IronPort Appliances Telnet Remote Code Execution Vulnerability』は、
http://tools.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20120126-

ironport にあります。

修正済みソフトウェアの入手

Cisco IronPort は Cisco IronPort E メール セキュリティ アプライアンスにおけるこの脆弱性を修正するソフトウェア アップデートをリリースしました。 このアドバイザリに記載された脆弱性の影響を受ける製品は、Cisco IronPort によって直接サポートされています。修正済みソフトウェアを入手するには、以下のリンクをクリックして Cisco IronPort テクニカル サポートにお問い合わせください。Cisco IronPort テクニカル サポートは、適切な修正済みソフトウェアの選択とインストール手順に関して、お客様をサポートします。保証に関するご質問はすべて、Cisco IronPort テクニカル サポートに直接お問い合わせください。

注：ソフトウェアのアップグレードに関し、psirt@cisco.com もしくは security-alert@cisco.com にお問い合わせいただくことはご遠慮ください。

http://www.ironport.com/support/contact_support.html

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 Center 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

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、適切な処置について支援を受けてください。

回避策の効果は、使用製品、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のお客様の状況に依存します。影響製品およびリリースが多種多様であるため、回避策を実際に展開する前に、対象とする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か、お客様のサービス プロバイダーやサポート会社にご相談ください。

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。

- +1 800 553 2447（北米内からのフリー ダイヤル）
- +1 408 526 7209（北米以外からの有料通話）
- 電子メール：tac@cisco.com

無償アップグレードの対象であることをご証明いただくために、製品のシリアル番号と、このアドバイザリの 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 を通して無償アップグレードをお求めください。

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

これらの Cisco IronPort アプライアンスに影響を与える *Telnet* サービスの脆弱性は、2011 年 12 月 23 日、FreeBSD プロジェクトによって公開されました。FreeBSD プロジェクトのアドバイザリについては、以下のリンクを参照してください。

http://security.freebsd.org/advisories/FreeBSD-SA-11:08.telnetd.asc

Cisco Product Security Incident Response Team（PSIRT）は、この脆弱性の影響を受ける Cisco IronPort アプライアンスを不正利用することが可能な Metasploit Framework のエクスプロイト モジュールを認識しています。

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。またシスコシステムズ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-20120126-ironport

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電子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

このアドバイザリに関する今後の更新があれば、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。このアドバイザリの URL で更新をご確認いただくことができます。

更新履歴

Revision 1.3	2012-February-08	Updated advisory to fix minor HTML formatting issue.
Revision 1.2	2012-February-07	Updated advisory to include the availability of IronPort software updates.
Revision 1.1	2012-January-26	Updated advisory to include the availability of a Cisco Applied Mitigation Bulletin.
Revision 1.0	2012-January-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支援、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について詳しく知るには、Cisco.com の http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html にアクセスしてください。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。