IronPort 暗号化アプライアンス/PostX および PXE 暗号化脆弱性

High

アドバイザリーID : cisco-sa-20090114-ironport

初公開日 : 2009-01-14 16:00

バージョン 1.0 : Final

回避策 : Yes

Cisco バグ ID :

CVE-2009-0055

CVE-2009-0054

CVE-2009-0053

CVE-2009-0056

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

IronPort PXE 暗号化は E メール 暗号化 ソリューションです受信 システムの Public Key Infrastructure（PKI）または特別捜査官のための必要なしで E メール通信を保護するように設計されている。 電子メール メッセージが暗号化がターゲットとなっているとき、IronPort E メール ゲートウェイの PXE 暗号化 エンジンは HTMLファイルとしてオリジナル電子メール メッセージを暗号化し、受信者に送られる通知電子メール メッセージに接続します。 HTMLファイル添付ファイルを復号化するのに使用される毎メッセージ キーがローカル IronPort 暗号化アプライアンス、PostX ソフトウェアインストーレーションか Cisco 管理されたソフトウェア サービスである Cisco Registered Envelope Service で保存されます。

PXE 暗号化プライバシー脆弱性

IronPort PXE 暗号化 ソリューションは不正 なユーザーがセキュア電子メール メッセージのコンテンツを表示することを可能にする可能性がある 2 脆弱性から影響を受けます。 脆弱性を不正利用するために、攻撃者は最初にネットワークのまたは妥協された電子メール アカウントによるセキュア電子メール メッセージを代行受信する必要があります。

IronPort 暗号化アプライアンス 管理インターフェイス脆弱性

IronPort 暗号化アプライアンス デバイスは許可されていないユーザが IronPort 暗号化アプライアンス 管理インターフェイスへのアクセス権を得、他のユーザの設定を修正することを可能にする可能性がある 2 脆弱性が含まれています。 これらの脆弱性は Cisco Registered Envelope Service ユーザに影響を与えません。

シスコはこれらの脆弱性に対処するソフトウェア アップデートを提供しています。 このアドバイザリに説明がある脆弱性のための回避策がありません。

このアドバイザリは http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090114-ironport で掲示されます。

該当製品

修正済みソフトウェア

次の IronPort 暗号化アプライアンス/PostX バージョンはこれらの脆弱性から影響を受けます:

- 6.2.1.1 以前の PostX すべての 6.2.1 バージョン
- 6.2.2.3 以前の PostX すべての 6.2.2 バージョン
- 6.2.4.1.1 以前のすべての IronPort 暗号化アプライアンス/PostX 6.2.4 バージョン
- すべての IronPort 暗号化アプライアンス/PostX 6.2.5 バージョン
- すべての IronPort 暗号化アプライアンス/PostX 6.2.6 バージョン
- 6.2.7.7 以前のすべての IronPort 暗号化アプライアンス/PostX 6.2.7 バージョン
- 6.3.0.4 以前のすべての IronPort 暗号化アプライアンス 6.3 バージョン
- 6.5.0.2 以前のすべての IronPort 暗号化アプライアンス 6.5 バージョン

IronPort 暗号化アプライアンスで動作しているソフトウェアのバージョンは IronPort 暗号化アプライアンス 管理インターフェイスの About ページにあります。

注: 顧客はどのソフトウェア修正プログラムが環境に適当であるか判別するために IronPort サポートに連絡する必要があります。 詳細についてはこのアドバイザリの修正済みソフトウェア取得のセクションを参照して下さい。

脆弱性を含んでいないことが確認された製品

IronPort C、M および S シリーズ アプライアンスはこれらの脆弱性から影響を受けません。 毎メッセージ キー 保持のためにローカル IronPort 暗号化アプライアンスを使用するために Cシリーズ アプライアンスが設定することができるが Cシリーズ アプライアンスは脆弱ではないです。 Cisco Registered Envelope Service は脆弱ではないです。

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。

改訂履歴

リビジョン 1.0	2009-January-14	初版リリース

利用規約

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も示唆するものではありません。 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、シスコは本ドキュメントの内容を予告なしに変更したり、更新したりする権利を有します。
本アドバイザリの記述内容に関して情報配信の URL を省略し、単独の転載や意訳を施した場合、当社が管理した情報とは見なされません。そうした情報は、事実誤認を引き起こしたり、重要な情報が欠落していたりする可能性があります。 このドキュメントの情報は、シスコ製品のエンドユーザを対象としています。