ネットワーキング機器の侵入に関するDer Spiegelの記事

アドバイザリーID : cisco-sa-20131229-der-spiegel
初公開日 : 2013-12-29 19:17
最終更新日 : 2014-03-13 18:56
バージョン 2.0 : Final
回避策 : No Workarounds available
Cisco バグ ID :

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

2013年12月29日、ドイツのニュース誌 Der Spiegelは、米国国家安全保障局(NSA)から漏洩した文書を参照して、ネットワークデバイスの「ソフトウェアインプラント」について言及した記事を公開しました。シスコは、この記事で言及されている多くのテクノロジー企業の1つです。

http://www.spiegel.de/international/world/catalog-reveals-nsa-has-back-doors-for-numerous-devices-a-940994.html

2013年12月30日、Cisco Product Security Incident Response Team(PSIRT)は、一部のCisco PIXおよびCisco ASAプラットフォームでインプラントが作成された疑いを調査するインシデントを開始しました。

シスコは、米国政府とドイツのニュース誌Der Spiegelの両方から、これらの申し立てに関する追加情報を正式に要請しました。これ以上の詳細は明らかにされていない。

Cisco PSIRTは、世界中のシスコのエンジニアリング、サポート、サプライチェーン組織と密接に協力しながら、Cisco ASAプラットフォームの包括的な評価を主導しました。Cisco PIXプラットフォームは サポート終了のため、Cisco ASAプラットフォームに重点を置きました。

調査(PSIRT-1384943056)では、シスコの開発およびサプライチェーンの手順、ASAおよびPIXプラットフォームに関するカスタマーサポートデータの履歴、および世界各地のさまざまな実稼働ネットワークに設置されているデバイスの運用データを確認しました。

Cisco ASAプラットフォームのBIOS、オペレーティングシステム、およびアプリケーションに焦点を当てた、さまざまなテストシナリオの作成と実装には、内部および外部の業界エキスパート

からのアドバイスが使用されました。世界中のシスコの専門家が、Cisco ASAファミリのすべての既存モデルのテストを実施しました。

BIOS、OS、アプリケーションの手順の異常や改ざんの証拠は見つかりませんでした。その結果、Cisco PSIRTはこの調査を終了しました。

追加情報

次のステップ：
シスコは、お客様がCisco ASAプラットフォームの整合性チェックを実行できるようにする機能の開発を続けています。完了すると、これらの機能は通常のシスコ製品リリースプロセスの一部としてCisco ASAソフトウェアに統合されます。

お客様に対するシスコの継続的な取り組みの一環として、すべての製品は定期的な侵入テストとセキュリティ評価の対象となります。テストおよび検査で判明した事項は、シスコの セキュリティ脆弱性ポリシーに従って伝達されます。これらの脆弱性は、社内テストの一環として発見されたり、お客様やその他の外部関係者からシスコに報告されたりする場合があります。

シスコでは、次のようなセキュリティおよび業界のベストプラクティスを推奨しています。

- 不具合およびソフトウェアの脆弱性に対処するための継続的なパッチ管理
- ネットワークデバイスの管理資格情報と物理アクセスの保護。
- ネットワークテレメトリの広範なネットワークモニタリングと分析を実施します。

セキュリティのベストプラクティスに関するお客様の追加情報については、https://sec.cloudapps.cisco.com/security/center/intelliPapers.x?i=55を参照してください。

また、シスコの セキュアな開発ライフサイクルと業界をリードする サプライチェーンオペレーションに関する追加情報もご覧いただけます。

ネットワーク管理業務を通じて疑わしいアクティビティや悪意のあるアクティビティを確認したお客様は、通常のサポートプログラムに参加し、Cisco PSIRTにエスカレーションすることをお勧めします。Cisco PSIRTの使用手順については、シスコのパブリック セキュリティ脆弱性ポリシーを参照してください。

シスコのセキュリティ手順

シスコ製品のセキュリティの脆弱性に関するレポート、セキュリティ障害に対する支援、およびシスコからのセキュリティ情報を受信するための登録に関するすべての情報は、シスコのワール

ドワイド ウェブサイト https://sec.cloudapps.cisco.com/security/center/resources/security_vulnerability_policy.html から入手できます。この情報には、シスコのセキュリティ通知に関して、報道機関が問い合せる場合の説明も含まれています。すべての Cisco セキュリティ アドバイザリは、http://www.cisco.com/go/psirt から入手できます。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20131229-der-spiegel

改訂履歴

バージョン	説明	セクション	日付
Revision 2.0	Cisco PSIRT調査が終了しました。		2014年3月13日
リビジョン 1.2	この記事で特定の脆弱性について説明または開示していないことを明確にするために、「シスコの対応」セクションを更新。		2013年12月30日
リビジョン 1.1	影響を受けたと思われるシスコプラットフォームの詳細が開示されたため、対応を更新。		2013年12月30日
リビジョン 1.0	初回公開リリース		2013-December-29

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。

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。