報道関係者各位

シスコ製スイッチの偽造品が市場に流通、エフセキュアが調査

～ システムコンポーネント認証プロセスを迂回するように設計された偽造品 ～

2020 年 7 月 16 日
エフセキュア株式会社

先進的サイバー・セキュリティ・テクノロジーのプロバイダである F-Secure (本社: フィンランド・ヘルシンキ、CEO: Samu Konttinen、日本法人: 東京都港区、以下、エフセキュア)は、シスコシステムズ製ネットワークスイッチの偽造品に関して同社のコンサルティング部門である F-Secure Consulting が行った調査に関するレポートを発表しました。調査の結果、偽造品はシステムコンポーネントを認証するプロセスを迂回するように設計されており、ハードウェアの偽造品がもたらすセキュリティの課題を示すものとなっています。

F-Secure Consulting のハードウェアセキュリティ チームは、Cisco Catalyst 2960-X シリーズスイッチの 2 種類の偽造品について調査を行いました。ソフトウェア更新の際に偽造品の機能が停止し、それによってユーザ企業が異変に気付きました。これは、偽造された／変更が加えられたデバイスが新しいソフトウェアに対して示す反応としてはよく見受けられるものです。顧客企業の依頼により、F-Secure Consulting は偽造品を徹底的に分析し、セキュリティ上の脅威を検証しました。

調査では、偽造品にはネットワークに対する攻撃を容易にするバックドアのような機能は備えていなかったものの、セキュリティ制御を回避するために様々な手段を用いていたことが判明しました。例えば、あるユニットでは、ゼロデイ脆弱性 (これまでに発見されていないソフトウェアの脆弱性) を悪用して、ファームウェアの改ざんに対する保護を提供するセキュアブートプロセスが弱体化させられていました。

F-Secure Consulting のシニアコンサルタントであり、今回の調査のリーダーを務めた Dmitry Janushkevich (ドミトリー・ヤヌシュケヴィッチ) は、次のように語っています。
「偽造品は認証手段を回避するように作られていることが判明しましたが、他のリスクをもたらすことを示す証拠は見つかりませんでした。偽造者の動機は偽造デバイスの販売によって利益を得ることだけに過ぎなかったようですが、これだけの技術を持った攻撃者ならば同様のアプローチを使用して企業にバックドアを仕掛ける可能性もあるため、こうしたデバイスの入念な調査は非常に重要となります。」

偽造品は、物理的にも動作的にも本物のシスコシステムズ製スイッチに酷似していました。デバイスのエンジニアリング上の特長の 1 つは、偽造者が正規品の元の設計を複製するために多額の投資を行ったか、またはユーザが正規品だと考えるに足りるだけの偽造品を製造するために、シスコシステムズのエンジニアリングドキュメントにアクセスした可能性のあることを示唆していました。

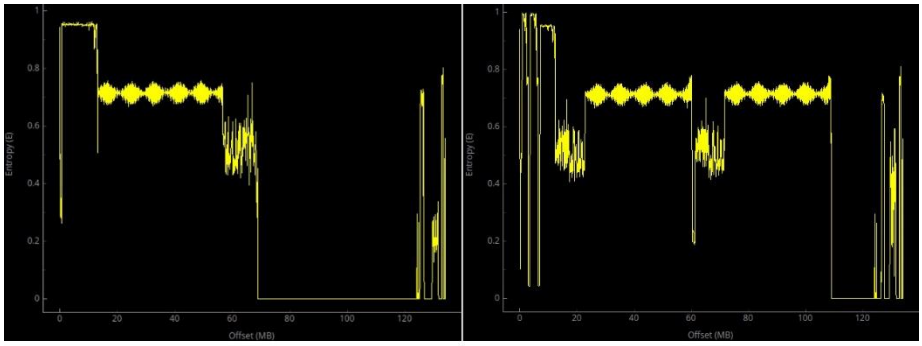
偽造品に搭載されている不明パーツ (U55)。
チップ上部のマーキングが消されている。

F-Secure Consulting のハードウェアセキュリティの責任者である Andrea Barisani (アンドレア・バリサニ) は、本レポートで分析されているような高度な偽造品が企業のセキュリティに対して与える大きな影響について、次のように話しています。
「企業のセキュリティ部門は、改ざんまたは変更されたハードウェアを無視することはできません。そのため、騙されて購入／使用してしまった偽造品は徹底的に調査する必要があります。ハードウェアを分解して最初から調査しないと、手を加えられたデバイスがセキュリティ面でどのような影響を与えたかを知ることができません。場合によっては、企業のセキュリティ／プロセス／インフラを保護することを目的としたセキュリティ対策が完全に損なわれてしまうほど大きな影響が発生する場合もあります。」

企業が偽造デバイス／コンポーネントを使用してしまうことを避けるための、エフセキュアからのアドバイスは以下のとおりです。

- 全てのデバイス／コンポーネントはメーカーの認定リセラーから調達する
- 調達プロセスを管理する明確な内部プロセスとポリシーを策定する
- 全てデバイス／コンポーネントが、メーカーが提供する最新の利用可能なソフトウェアを実行していることを確認する
- 同じ製品の複数ユニット間において物理的な違いを発見した場合、それが微妙な違いであっても全て記録する

「エフセキュアは知的財産の保護とファームウェア／ハードウェア製品の信頼性の確保に不可欠なセキュアブートスキームの侵害と実装に関する、世界のリーディングカンパニーです。今回のようなケースに対する詳細な分析により、偽造品がセキュリティに与える影響を判断する上での課題だけでなく、疑わしいデバイスを発見した顧客をどのようにサポートし、安心していただくことができるかがよくわかりました。」と、バリサニは締めくくっています。



純正品ユニット (左) と偽造品ユニット (右) のフラッシュイメージのエントロピーグラフ

今回の調査レポートは以下のページにてご覧いただけます (英語)。
https://labs.f-secure.com/publications/the-fake-cisco

F-Secure Consulting は 4 大陸 11 ヶ国に拠点を構え、銀行、金融サービス、航空、海運、小売、保険、その他セキュリティがクリティカルとなる分野において、高度なサイバーセキュリティコンサルティングサービスを提供しています。
https://www.f-secure.com/en/consulting (英語)

プレスリリース掲載ページ:
http://jp.press.f-secure.com/2020/07/16/cisco-counterfeit-jp/

エフセキュアについて

エフセキュアほど現実世界のサイバー脅威についての知見を持つ企業は市場に存在しません。数百名にのぼる業界で最も優れたセキュリティコンサルタント、何百万台ものデバイスに搭載された数多くの受賞歴を誇るソフトウェア、進化し続ける革新的なセキュリティ対策に関する AI テクノロジー、そして「検知と対応」。これらの橋渡しをするのが

エフセキュアです。当社は、大手銀行機関、航空会社、そして世界中の多くのエンタープライズから、「世界で最も強力な脅威に打ち勝つ」という私たちのコミットメントに対する信頼を勝ち取っています。グローバルなトップクラスのチャネルパートナー、200 社以上のサービスプロバイダーにより構成されるネットワークと共にエンタープライズクラスのサイバーセキュリティを提供すること、それがエフセキュアの使命です。
エフセキュアは本社をフィンランド・ヘルシンキに、日本法人であるエフセキュア株式会社を東京都港区に置いています。また、NASDAQ ヘルシンキに上場しています。詳細は https://www.f-secure.com/en/welcome (英語) および https://www.f-secure.com/ja_JP/ (日本語) をご覧ください。また、Twitter @FSECUREBLOG でも情報の配信をおこなっています。

※以下、メディア関係者限定の特記情報です。個人の SNS 等での情報公開はご遠慮ください。

【本件に関する報道関係者からのお問合せ先】

エフセキュア株式会社
広報部　　秦　和哉
TEL：03-4578-7745 (直通)　　japan-pr@f-secure.com