文中のハイパーリンクは英文のサイトとなっております、日本語をご希望される場合はブラウザの翻訳機能等をご使用ください。

ICTサプライチェーンで弱点となるファームウェア

はじめに

今日、組織内のすべての情報通信技術（ICT）機器は、ベンダーやサプライヤーの複雑な製造連携によるチップ、コンポーネント、コードの集合体です。この複雑な技術サプライチェーンのどのリンクも、資産と取得する組織全体のセキュリティを損なう可能性のある脅威や脆弱性をもたらす可能性があります。これらの負の資産として継承されているリスクを管理するために、ITおよびセキュリティチームは、ファームウェア・エコシステムという、しばしば不慣れな領域に目を向けることを余儀なくされます。

デバイスファームウェアは、あらゆる種類のデバイスに組み込まれた重要なソフトウェアです。2022年2月に米国商務省と国土安全保障省が発表した共同レポート「米国の情報通信技術産業を支える重要なサプライチェーンの評価“Assessment of the Critical Supply Chains Supporting the U.S. Information and Communications Technology Industry”」では、サプライチェーンにおけるファームウェアのセキュリティの必要性が明確に訴えられています。また、Security Weekの記事は、「米政府、ファームウェアのセキュリティを‘シングル・ポイント・オブ・ファーラー’と指し厳しい警告を提唱。“U.S. Government Issues Stark Warning, Calling Firmware Security a ‘Single Point of Failure’“」という見出しで、この報告書を要約しています。

SECURITYWEEK
CYBERSECURITY NEWS, INSIGHTS & ANALYSIS

U.S. Government Issues Stark Warning, Calling Firmware Security a ‘Single Point of Failure.’

報告書自体も、サプライチェーンのリスクに関するセクションの最後に、明確な警鐘を鳴らしています：

"ファームウェアは、電子機器の数が増え、ICTサプライチェーンが複雑化するにつれて、大規模かつ拡大し続ける攻撃対象になっています。"

Assessment of the Critical Supply Chains Supporting the U.S. Information and Communications Technology Industry

2022年2月付けの米国商務省および米国国土安全保障省による報告書

なぜ、ここに注目するのでしょう？エンドユーザーのラップトップ、ネットワーク機器、ローカルまたはクラウド上のサーバーなど、他のすべてのテクノロジーは、最終的に物理的な機器に依存しています。そして、これらすべてのデバイスの中に、ファームウェアが広く存在しているのです。ファームウェアは、デバイスや物理コンポーネントが実際にどのように動作するかを管理する、永続的なロジックなのです。もしデバイスがこのレベルで侵害された場合、デバイス上の上位層のデータ、アプリケーション、およびサービスはすべて危険にさらされることになります。

サプライチェーンのリスクに関して言えば、ファームウェアとハードウェアの緊密な統合と依存関係が、最悪な関係を作り出しています。物理デバイスは、多くの生産される国にまたがる、圧倒的に深いサプライチェーンを有しており、外部の敵や悪意のある内部関係者によるミスや侵害の機会を多く作り出してしまっています。ファームウェア・パッケージは、多くのサプライヤーによって再利用されることが多いため、あらゆる脆弱性が数え切れないほどの製品に影響することになります。ソフトウェアと同様に、ファームウェアも、デバイスがデプロイされた後でも、サプライ・チェーンが侵害されることを防ぐために、しばしば定期的なアップデートを必要とします。そして、これらのリスクはすべて、ベンダーやデバイスの種類の数だけ、独自のサプライチェーンとリスクを持つことになります。

このリスクを軽減するためには、企業は、デバイスやコンポーネントの信頼性、完全性、動作を、ファームウェアレベルまで独自に検証できなければなりません。ファームウェアに到達することによってのみ、組織は、自分たちの技術が本当に想定通りのものであることを、真に検証することができるようになるのです。このためには、新しいプロセスやツールが必要かもしれませんが、これは、サプライチェーンのリスクマネジメントの不可欠な部分なのです。

本書は、サプライチェーンリスクマネジメント（SCRM）やサプライチェーン保証の要素を含む、サプライチェーンセキュリティのファームウェアとハードウェアの側面について、詳細な見識を提供するものです。これは、以下のような相互に関連する様々なトピックをカバーするものです。

- 実際のサプライチェーンにおける攻撃と傾向
- サプライチェーンリスクの全体像におけるファームウェアの位置づけ
- サプライチェーン・アタックにおけるファームウェアの役割
- ファームウェアのサプライチェーンセキュリティのためのプラクティス

現実のサプライチェーンにおける攻撃とその傾向

サプライチェーンへの攻撃はここ数年で顕著に増加しており、民間企業だけでなく政府機関にも影響を与えています。2021年のクラウドストライクの調査では、45%の組織が過去12ヶ月間に少なくとも1回のサプライチェーン攻撃を経験しており、セキュリティ企業のSonatypeは、サプライチェーン攻撃が430%も増加したと報告しています。

このようなサプライチェーン攻撃の増加は、様々な要因に起因しています。まず、組織内部のサイバーセキュリティ対策が改善されたことで、サプライチェーン攻撃は、攻撃者の標的をより脆弱なサプライチェーンの上流にシフトさせようとします。これにより、攻撃者は、標的の組織に届く前にデバイスやコードを危険にさらすことができるだけでなく、組織が技術パートナーに対して持つ固有の信頼性を利用することができます。また、サプライチェーン攻撃は「一対多」の感染経路を提供し、1つの侵害が数百または数千の下流組織に広がる可能性があります。さらに、Covid-19の大流行により、OEMやテクノロジープロバイダーは世界的な供給不足とサプライチェーンの混乱への対応を迫られ、サプライチェーンにさらなる流動性をもたらしています。このため、攻撃者がサプライチェーンに入り込む機会がさらに増えています。

サプライチェーンへの攻撃は一般的になってきましたが、数年前からよく知られるようになり、ほとんどの場合、高度な攻撃をする攻撃者と関連しています。Breaking_Trustプロジェクトは、過去数年間に公にされた139件のサプライチェーン攻撃の記録を一元管理しています。最もよく知られた例としては、以下のようなものがあります:

- SolarWinds SUNBURST - 高度な攻撃者がSolarWindsに侵入し、Orionとして知られるSolarWindのIT Monitoring and Managementプラットフォームのソースコード内に悪意のあるコードを埋め込むことに成功しました。侵入されたコードは、その後正式リリースされてしまい、様々な大手テクノロジー企業を含む18,000以上の連邦政府および民間企業の顧客へ配信されました。攻撃者は、IT管理ツールに感染することで、機器のファームウェアを更新する機能を含む、さまざまなサーバーや資産を危険にさらす機会を得てしまいました。

- ASUS ShadowHammer - 攻撃者は、ASUS Live Update Utilityを改変し、適切に署名されていながら悪意のあるアップデートを57,000人以上のユーザーに配信することが可能でした。Live Update Utilityは、ソフトウェア・アップデートに加えて、BIOSおよびUEFIのアップデートも提供するため、特に重要で、攻撃者は潜在的に悪意のあるシステム・ファームウェアを配信できるようになりました。

- CCleaner - セキュリティ会社Avastの人気ユーティリティCCleanerにバックドアを追加されてしまいました。同ソフトウェアのビルド環境を侵害することで、攻撃者は悪意のあるコードを挿入することができ、最終的に220万人以上のユーザーに配信されました。

これらは、実際に観測された多くのサプライチェーン攻撃のうちのほんの一部に過ぎません。しかし、これらはすべて、サプライチェーンが企業内の最も重要な領域や資産への信頼できる侵入経路となり得ることを明確に示しています。

サプライチェーンリスクの全体像の中のファームウェア

テクノロジーのサプライチェーンには様々な形態がありますが、最終購入者側からの視点から見ると、サプライチェーンのリスクは、機器、アプリケーション、サービスという3つの基本的なソースに分けることができます。この3つのカテゴリーはすべて、現実の脅威のベクトルとして利用されてきました。同様に、これら3つはすべて、技術を最初に取得したときだけでなく、運用中のライフサイクルにおいても、サプライチェーンリスクを引き起こす可能性があります。

組織の機器やデバイスを見ると、長期的なリスクのほぼすべてがファームウェアに結びついています。さらに、物理的な機器やデバイスのファームウェアを見たとき、サプライチェーンリスクを引き起こす根本的な要因の多くは、拡大されます。例えば、物理的なデバイスは、最も多層なサプライチェーンを持ち、最も多くのコンポーネント生産国にまたがっています。ファームウェアレベルでは、コードの再利用が一般的であり、新たな脆弱性が発見された場合、極めて広範な問題を引き起こす可能性があります。そして、当然のことながら、機器とそのファームウェアは、環境において、最も広範に展開され、 価値の高い資産の一部であり、最も影響力の高いテクノロジーのひとつとなっているのです。

さまざまなリスク要因とその要因について議論するとき、すべてをソフトウェアに照らし合わせて見たくなるものです。「それはすべて、ある種のコードです。ではファームウェアは、どう違うのだろうか？→すべて同じ問題です。」特に、防御者は、アプリケーションやOSを修正し、ハードニングするスキルを身につけていますが、攻撃者は、セキュリティチームがファームウェアを防御するよりも、ファームウェアを武器にすることに不釣り合いなほど熟練しているという意味で、異なっているというスタンスをとっています。

このような観点から、テクノロジー・サプライチェーンの3つの主要なカテゴリーを詳しく見てみましょう。

リスク要因	機器デバイス	アプリケーション	サービス
サプライチェーンの階層	とても高い	中程度	低い
生産された国	高い	高い	低、もしくは中
関係ベンダー数	中、もしくは高	高い	低い
コードの再利用	高い	高い	低い
攻撃のインパクト	とても高い	高い	とても高い

Eclypsiumによる、さまざまなサプライチェーンの層におけるリスクレベルの評価

マネージドサービス

マネージド・サービス・プロバイダーは、サービスを提供するために、通常、お客様の環境に特権的にアクセスする必要があります。サービスプロバイダが侵害された場合、攻撃者はこの信頼関係を悪用して、サービスプロバイダの下流に位置する顧客を危険にさらすことができます。この戦略は、ランサムウェアのギャングに特に人気があり、有名なKesaya攻撃では、攻撃者がサービス会社を利用して、最大1,500の企業にランサムウェアを感染させたことが知られています。サービスプロバイダは、顧客企業の機密性の高いシステムやインフラにアクセスすることができるため、こうした攻撃は非常に広範囲に及び、組織に影響を及ぼす可能性があります。

唯一の朗報は、ほとんどの組織では、自社のテクノロジーやインフラにこのレベルでアクセスできる信頼できるプロバイダーの数が非常に限られていることです。また、サービスプロバイダーは自己完結型で、他のベンダーに委託するのではなく、自社で直接サービスを提供しています。このような特徴は、攻撃者がサービス・プロバイダーにアクセスする機会を制限することができます。

アプリケーションとソフトウェア

サードパーティーのアプリケーションやソフトウェアは、当然ながら組織のテクノロジーの大部分を占め、同様にサプライチェーンリスクも高くなります。アプリケーションのサプライチェーンリスクに関する最も顕著な問題の1つは、ほとんどの組織が多くのアプリケーションベンダーと取引をしていることです。これらのベンダーのいずれかが、外部の敵や悪意のある内部者によって侵害される可能性があり、また、そのコードに既知または未知の脆弱性を持ち込む可能性があります。アプリケーションサプライチェーンリスクのもう一つの最も一般的な原因は、オープンソースソフトウェアとプロジェクトの再利用に起因します。これらのオープンソースライブラリに存在する脆弱性は、ベンダーのアプリケーションに引き継がれ、大規模な情報漏洩につながる可能性があります。

しかし、オープンソースプロジェクト以外では、ほとんどのアプリケーションのサプライチェーンは特に深くありません。ベンダーは自身のコードベースに責任を持ち、仲介業者を介して販売される場合でも、コードはベンダーのサーバーから直接配信されることが多くなっています。このため、少なくとも、サプライチェーンの問題を引き起こす可能性のある関係者の数は限られています。

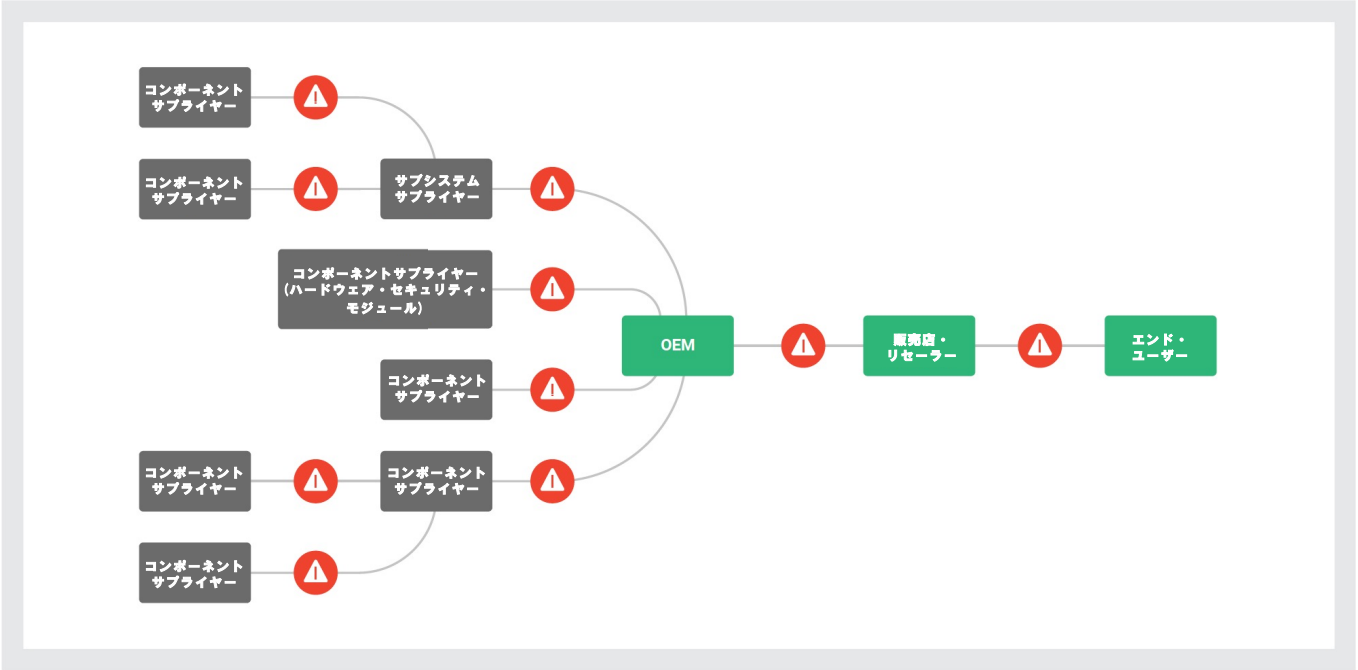
アプリケーションは定期的に更新される必要があり、更新コードや更新プロセスを侵害することは、アプリケーションのサプライチェーンにおける最も一般的なベクターの1つであることが証明されています。SolarWindsの攻撃はその1例で、敵対者はSolarWindsに侵入し、通常の製品アップデートを通じて配信されるソースコードにアクセスすることができました。組織がさらされる範囲は、当然ながら、アプリケーションの性質によって大きく異なります。多くの場合、危険にさらされるのは、アプリケーションに含まれるデータの盗難や損失に限定されるかもしれません。しかし、他の多くのシステムと相互作用するアプリケーションは、攻撃者が他の内部資産に拡散することを可能にするかもしれません。しかし、最も重要なソフトウェアサプライチェーン攻撃の1つが、攻撃者に組織の重要なインフラストラクチャと機器へのアクセスを可能にするソフトウェアであったことは、偶然ではありません。

デバイスファームウェア

物理的な機器やインフラのサプライチェーンは、間違いなく最も複雑で、最もリスクが高く、そのリスクのほぼすべてがファームウェアに関連しています。デバイス・ファームウェアは、オペレーティング・システムの下に位置し、デバイスとその中の事実上すべてのコンポーネントの実際の機能を制御する、統合されたロジックです。IoTデバイスのような多くのデバイスは、ファームウェアのみを搭載しています。ネットワーク機器のような他の種類の機器は、統合されたファームウェアや、 ハードウェアと緊密に統合され

高度にカスタマイズされたオペレーティングシステムに大きく依存しています。また、企業は通常、新しいサーバーやノートパソコンに独自のOSイメージをインストールしますが、ファームウェアは変更されないままであることがよくあります。つまり、デバイスが実際にどのように動作するかを管理するのはファームウェアであり、永続するのはデバイス内のファームウェアなのです。

アプリケーションやサービスとは異なり、物理的なデバイスには非常に深いサプライチェーンがあり、頻繁に変更されます。1つのデバイスには、数百もの特殊なコンポーネントやシステムがあり、多くの国にまたがる数十のサプライヤーやサブサプライヤーが関与していることがあります。サプライヤーの選定は、セキュリティ上の懸念ではなく、コストや供給力の圧力に基づいて行われることがよくあります。また、最近の重要部品の供給不足のような状況の変化に対応するために、OEMは新しいサプライヤーに迅速に移行する必要がある場合もあります。これらの多くの可動部品のいずれかに脆弱性、外部からの攻撃、または悪意のある内部者が存在すると、デバイス全体の整合性が危険にさらされる可能性があります。



また、アプリケーションと同様に、ファームウェアもコードの再利用により定期的に危険にさらされています。プロプライエタリおよびオープンソースのファームウェア・コンポーネントは、様々なベンダーによって定期的に使用されており、脆弱性は、何十ものベンダーに影響を与える可能性があることを意味します。例として、いくつかの主要な機器ベンダーが、共通のファームウェアSDKに関連するUEFIの脆弱性の影響を受けています。同様に、一般的に再利用されているTCP/IPスタックに存在するRipple20の脆弱性は、数十のベンダーに渡っています。しかし、より重要なことは、これらのファームウェアレベルの脆弱性は単なる理論上のものではなく、急速に、そして活発に悪用されているということです。

- HPは最近、Integrated Lights Out管理インターフェイスのアクティブエクスプロイトに関連する16の影響力の大きいUEFIファームウェアの脆弱性に緊急パッチをリリースしました。
- CISAは今月初め、Ciscoルーターの約60の脆弱性を狙ったアクティブエクスプロイトについて警告しました。
- Ars Technicaは、今年2月に「Russia's most cutthroat hackers infect network devices with new botnet malware（ロシアで最も悪辣なハッカーがネットワーク機器に新たなボットネットマルウェアを感染させる）」という見出しで、ファイアウォールに対するCyclops Blink攻撃に言及し、ファームウェアエクスプロイトについて記事を書いています。

また、組織は当然ながら様々なベンダーから機器を購入することになる。ノートパソコンもサーバーもネットワークインフラも、当然ながら非常にユニークなサプライチェーンを持っているはずです。しかし、同じベンダーの製品であっても、モデルごとに、あるいは同じモデルでも世代ごとに異なることがあります。そして最後に、機器のサプライチェーンの侵害は、影響と範囲の点で特に大きなダメージを与える可能性があります。内蔵された脆弱性や脅威は、当然ながら類似の機器に共有されるため、組織の全機器が危険にさらされる可能性があります。また、デバイス上の最も特権的なコードにアクセスできるため、攻撃者はデータの窃盗からステルス性の確立、デバイスやインフラの永久的な無効化まで、ほぼすべての悪意ある行為を自由に行うことができます。

最後に、物理的な機器とそのファームウェアは、サプライチェーンの他の側面の論理的な基盤であるこ とを指摘しておきます。どのようなアプリケーションやサービスも、最終的にはハードウェア上で実行されます。もし、基盤となるインフラストラクチャが侵害された場合、より高いレイヤーのセキュリティが疑われるか、高リスク環境では、完全に失われることになります。

サプライチェーン・アタックにおけるファームウェアの役割

ファームウェアは、デバイス上で最初に実行されるコードであり、カーネルの「下」に位置することから、最も特権的なコードの一部でもあります。これらの特性は、当然ながら、サイバー攻撃の多くの局面において、攻撃者にとってファームウェアを非常に価値のあるものにしています。攻撃者がファームウェアを使用し、悪用する多くの方法についての完全な分析は、この文書の範囲外ですが、サプライ・チェーン攻撃において、ファームウェアが特に使用される最も一般的な方法のいくつかを 確認してみましょう。

初期アクセスベクトル

ファームウェアは、敵対者に組織への初期アクセスを提供するために、様々な方法で悪用される可能性があります。最も直接的なのは、ファームウェアのインプラントやバックドアを、最終的な顧客に引き渡される前に、製品へ導入することである。このようなインプラントは、非常に基本的なもので、追加の悪意あるコードやペイロードをダウン ロードできる、デバイス内の信頼された足場を提供するだけである場合があります。このような小さなコードの断片は、既存のファームウェアに簡単に追加したり、ファームウェア・メモリの未使用領域や「コードケーブ」に格納したりすることができます。

インプラントは、いくつかの方法でファームウェアに導入される可能性があることに留意することが重要です。当然ながら、攻撃者やサプライヤー内の悪意あるインサイダーは、ファームウェアにバックドアを ソースから直接挿入することができてしまいます。しかし、他のサプライヤーのファームウェアを修正するために、サプライチェーン内の事実上あらゆる主体が、広範な脆弱性を悪用することが可能なのです。これらの同じコンセプトは、ファームウェアのアップデートにも適用され、攻撃者は、ソース・ベンダーを 直接侵害することも、安全でないアップデート・プロセスを利用することも可能なのです。

しかし、サプライチェーン内の脆弱性は、製品が納入された後に、攻撃者に容易な感染経路を提供することができ、これは、現実の攻撃において最も一般的な経路の1つであることが証明されています。VPN、ファイアウォール、ルーターなどのネットワーク機器に存在する脆弱性は、国家が支援する高度な攻撃者にとっても、最も人気のあるランサムウェア集団にとっても、人気のある初期感染経路のひとつとなってしまっています（PDF）。

パーシスタンシー

また、ファームウェアは、ドライブやオペレーティング・システムの領域を超えて、デバイス上の位置を維持する方法を敵に提供します。これにより、脅威が検出され、デバイスが完全に消去、再インストール、またはシステム・ドライブの交換された場合でも、攻撃者は容易に回復することができます。最近のiLOBleed攻撃は、脅威が最初に検出された後、攻撃者がHPEサーバーをランサムウェアに再感染させ、感染したシステムを再イメージ化することを繰り返した実例です。

このようなレベルのパーシスタンシー（持続性）は、サプライチェーン攻撃の流れの中では特に重要です。結局のところ、攻撃者のコードがすぐに更新され、上書きされてしまうのであれば、サプライチェーンを侵害する意味はないのです。ファームウェアは、高い特権と長い寿命を持つコードにアクセスすることができてしまいます。

防御回避

攻撃者は、セキュリティツールからの検知を避けるために、ファームウェアを利用することもできます。ほとんどの既存のセキュリティ・ツールは、ファームウェアに関する専門知識の継続的な提供と、問題を確実に検知するために必要な適切な能力を欠いています。これは、脆弱性とリスク管理、そして、脅威の検知という点で、盲点となります。

さらに、ファームウェアは、オペレーティング・システムとそれに依存するセキュリティ・ コントロールを破壊することができる、他に類を見ない強力なポジションに位置しています。例えば、悪意のあるファームウェアやブートローダは、攻撃者がシステムの起動方法を制御したり、機能を無効

化するためにオペレーティングシステムに直接パッチを適用することさえ可能にしてしまいます。悪意のあるファームウェアは、オペレーティングシステムに誤った情報を報告し、従来のセキュリティツールでファームウェアを確実に可視化することが難しくなります。再び、iLOBleed攻撃の例を挙げると、ファームウェアが、脆弱なバージョンを保持しているにもかかわらず、ファームウェアが正常にアップデートされたと偽って報告することがあるのです。もう一度言いますが、これらの特徴はすべて、ほとんどの組織が依存している保護機能を攻撃者が制御することを可能にするため、サプライチェーン攻撃において特に関連性が高いのです。

影響範囲

最終的にファームウェアは、データを盗んだり破壊したり、デバイス自体を完全に使用不能にすることで、組織に甚大な損害を与えることができてしまいます。そして、データを簡単に復元できるソフトウェア・レベルの攻撃とは異なり、ファームウェア・レベルでデバイスを無効化すると、機器に恒久的なダメージを与えたり、回復に多大な時間とリソースを要したりする可能性があります。さらに、サプライ・チェーン・アタックが組織のデバイス群全体に影響を与える可能性があるため、もしそのようなことになれば組織の業務維持能力に壊滅的な影響を与えます。

ファームウェアのサプライチェーンセキュリティのためのベストプラクティス

組織は、すべての重要な機器やデバイスの真正性、姿勢、完全性を確認できる必要があります。また、強力なサプライチェーンセキュリティプログラムは、デバイスの初期評価、取得、継続的な運用に至るまで、製品のライフサイクル全体を通じて拡張されることになります。従来のセキュリティ・ツールの多くがファームウェアに対する洞察力を欠いていることから、企業は、自社のデバイスを適切に評価するために、新しいプロセスやツールを開発する必要がある場合があります。ファームウェア・セキュリティ・プラットフォームは、最も重要なタスクの多くを自動化し簡素化することができますが、これらは、信頼できるサプライチェーン・セキュリティ・プログラムを達成するために明示的に要求されるものではありません。

主なステップとベストプラクティスは以下の通りです。

1. 識別：独立したファームウェアの可視化と検証の確立

サプライチェーンのセキュリティには、独立した第三者による可視化と検証が生来必要であり、特にファームウェアに ついては、それが顕著に現れます。テクノロジー・ベンダーは、当然、サプライチェーンのセキュリティにおいて重要な役割を担っていますが、ベンダー自体が危険にさらされている可能性がある以上、顧客は、ベンダーに依存して、自らの完全性を検証することなどできないのです。

そのため、組織は、ベンダーが納入する製品が本物であり、サプライチェーンの中で改変されていないことを検証するための技術的なツールを保有している必要があります。以下の技術的なステップとプロセスはすべて、デバイスのファームウェアを測定・分析し、脆弱性、脅威、 あるいは改ざんの兆候を特定する能力に依存しています。

2. 検証: 異なる3つのフェーズで検証を自動化する

検証は最も重要なステップの一つであり、購入前の計画から展開、そして継続的な監視に至るまで、3つのユニークな活動フェーズに分けることができます。

2.1 購入前の機器の脆弱性評価

ITおよびセキュリティチームは、選定プロセスの一環として、すべてのデバイスとコンポーネントに既知の脆弱性と設定ミスがないかを分析する必要があります。信頼できるベンダーは、自社の製品およびその基盤となるすべてのコンポーネントに弱点がないことを確認する必要があります。また、ベンダーは、製品に含まれるファームウェアのソフトウェアビルドオブマテリアル（SBOM）を提供しているかどうかを評価する必要があります。これらのSBOMは、デバイスに含まれるファームウェアの明確な報告であり、後にデバイスが最終的に納品される際に、スタッフが参考資料として使用することができます。

さらに、OEMは、さまざまな低レベルのデバイス構成とセキュリティ設定が適切に有効化され、連携して動作していることを確認する必要があります。例えば、Secured-Core PCの場合、OEMは、System Guard、System Management Mode、TPM(Trusted Platform Module)など、複数のベンダーの様々な技術を適切に統合する必要があります。小さな設定ミスや間違いが、予期せぬ形で簡単にシステムを危険にさらす可能性があります。可能であれば、ベンダーのファームウェア・アップデート・プロセスに、署名入りファームウェアを要求しないとか、アップデート・トラフィックを平文で送信するといった弱点がないかの評価も含まれるべきです。

ファームウェアセキュリティプラットフォームは、これらおよび他の多くの脆弱性と弱点について、将来のデバイスを簡単にスキャンできます。これにより、各ベンダーと安全な製品を提供するためのベンダーの取り組みに対する重要な洞察が得られ、自社のサプライチェーンのセキュリティを検証することを可能とします。

2.2 ファームウェアの脆弱性と脅威に対するすべての新規資産のスキャン

組織は、信頼できるベンダーと取引する場合でも、新たに入手したすべてのデバイスのファームウェアレベルまでの完全性とセキュリティ姿勢を検証することが重要です。サプライヤーやコンポーネントは定期的に変更される可能性があり、新たな脆弱性や脅威をもたらす可能性があります。また、デバイスは、倉庫保管、付加価値再販業者、物流・配送プロセスなど、メーカーを離れた後に改ざんされる可能性もあります。

脆弱性のスキャンに加えて、分析では、受け取ったすべてのファームウェアが、ベンダーやコンポーネント・サプライヤーから入手可能な公開ファームウェアと暗号的に一致していることを検証する必要があります。同様に、スキャンは既知のファームウェアの脅威に対するチェックを含むべきです。脅威が進化しても、攻撃者は、Hacking Team UEFI インプラントのコンポーネントを再利用した最近のMosaicRegressorインプラントに見られるように、以前のファームウェアの脅威のコンポーネントを再利用することがよくあります。

この分析は、どのように入手したかに関わらず、すべてのデバイスとアップデートに適用される必要があります。例えば、新しいラップトップがリモートユーザーに直接送られたとしても、デバイスの完全性を確保するために、そのデバイスをリモートでスキャンまたは評価する必要があります。同様に、M&A の結果として取得した機器もスキャンする必要があります。

2.3 すべてのアップデートを継続的に評価し、既存のデバイスの挙動を監視する。

ベンダーやサプライヤーが攻撃者に侵害された場合、悪意のあるコードが、適切に署名された、一見すると「有効な」コードとしてベンダーから配信される可能性は十分にあります。ファームウェアをベンダーの承認済みホワイトリストと比較するだけでは、脅威は「承認済み」バ ージョンの中に組み込まれているため、当然ながら脅威を明らかにすることはできません。

そのため、企業は、ファームウェアを入手した後、あるいはアップデートした後にも、その挙動を継続的に監視する必要があります。他の多くのソフトウェアと異なり、ファームウェアは、その挙動が非常に予測しやすい傾向にあるため、悪意ある行動が目立ちやすいのです。セキュリティ・チームは、既知の悪意のあるドメインにアクセスするような、明らかな悪意ある行動を 検出することができるかもしれません。一方、より巧妙な方法では、ファームウェア・セキュリティ・ プラットフォームが必要になるかもしれません。しかし、UEFI、BMC、インテルの AMT などのコンポーネント内のファームウェアは、ホスト OS からは見えない独自のネットワークスタックを持ち、ファームウェアの動作を直接監視することが重要であることに注意しなければなりません。

3. サプライチェーン全体でファームウェアのパッチとアップデートを実施する。

先に挙げた商務省・国土安全保障省の合同報告書で指摘された重大な問題のひとつに、重要なファームウェアの更新やパッチ適用が行われていないことがあります。

“ファームウェアのアップデートは、多くの企業にとって物流上の大きな課題となっています。多くの場合、デバイスのファームウェアは一度も更新されていないか、緊急時にのみ更新される可能性があります。”

なぜでしょうか？政府報告書によると、ファームウェアの更新プロセスは決して単純なものではありません。「例えば、特定のデバイスの最新のファームウェア・アップデートが何であるかが明確でない場合がある。その結果、ユーザーは機器のファームウェアが最新であるかどうかをすぐに判断できない可能性がある。暗号的に署名されておらず安全ではないファームウェアを持つデバイスの場合、デバイスは、署名されていないコードでアップデートされるかもしれない。つまり、ユーザーからの検証を必要とせずに、ファームウェアが書き換えられる可能性がある。かつて信頼されていたデバイスが、暗号化されていないアップデート後に、安全であると信頼されなくなる可能性がある。」

ファームウェアのアップデートに際しての支援は、組織として明らかに必要です。その支援には、アップデートを必要とするコンポーネントを探し出し、それを置き換えるための、検証された信頼できるアップデート・バイナリを見つけることが含まれる必要があります。また、Microsoft SCCM や Intune などの標準的な IT 自動化ツール、Tanium などの資産管理ソリューション、OSQuery などのエンドポイント可視化ソリューションとの緊密な統合も必要です。

「クラウド」につきましては「他人のハードウェア」に過ぎないことを念頭に置き、現代のICTサプライチェーンにはAWS、Azure、Google Cloudなどのクラウドプラットフォームも含まれていることを常に念頭に置く必要があります。そのため、企業は、ファームウェア・セキュリティ・ソリューションが、これらの主要なクラウド・プラットフォームの下にあるハードウェアと統合する豊富なAPIを備えている必要があるのです。クラウドプラットフォームの下にあるファームウェアのアップデートパスを保証することによってのみ、 私たちは、サプライチェーンを保証することができるのです。

結論と次のステップ

テクノロジーのサプライチェーンは複雑であり、相互依存性の高い暗黙の信頼のネットワークに依存しています。これらの機器の「DNA」として機能する何百万行ものファームウェアの完全性とリスクを独立して検証する能力がなければ、組織のセキュリティ・プログラム全体が、最も不安定な基盤の上に構築されることになってしまいます。

このようなリスクに対処するために、組織は、サプライチェーンのセキュリティを常に独立して評価できるようにする必要があります。ファームウェア・セキュリティ・ツール（ファームウェア・コードを特定、検証、強化するツール）は、これらの取り組みを徹底的、簡単、かつ一貫して行うための重要な役割を担っています。これにより、企業は、暗黙の信頼に頼ることなく、問題が発生する前に、積極的に技術を検証し、リスクを軽減することができるのです。

詳細については、eclypsium.com/ja/をご覧ください。