国家のサイバーセキュリティの改善について

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。

2021年のサイバーセキュリティ大統領命令：ゼロ・トラスト、サプライチェーンにおけるファームウェア、そしてデバイスの安全確保の要求

5月12日の国家のサイバーセキュリティの改善に関する大統領令は、サイバー攻撃の防止に向けた新たな視点と方向性を示す重要な文書です。大統領令の2つのセクションは、連邦政府機関のサイバーセキュリティチームに対する明確な義務としてだけでなく、新しい攻撃者の戦術に対抗するために戦略をレベルアップする必要がある民間チームにとっての革新的で新しいアプローチとしても非常に意義深いものとなっています。

1. セクション3は、”連邦政府のサイバーセキュリティの近代化”を求めており、特に政府ネットワークにおけるゼロトラストアーキテクチャの設計と実装に焦点を当てています。

2. セクション4は、ソフトウェアサプライチェーンの強化と保護に重点を置いています。

大統領令の10のセクションはすべて、連邦政府機関への明確な指示と各民間企業のCISOに対する前向きなガイダンスとして取り上げられますが、これら2つのセクションは、以前のベストプラクティスからの大きく変更されています。また、**セキュリティアーキテクト、アナリスト、脅威チームがデバイスの安全性を確立する上でファームウェアの役割を真剣に受け止める必要性も強く推奨しています。**

セクション3：大統領命令におけるゼロトラストアーキテクチャ

いくつかの重要なポイントの中で、大統領命令は、CISO、セキュリティアーキテクト、および実務担当者からの注意を喚起する以下のような一連のロジックに留意します：

- サイバーセキュリティプログラムを成功させるには、ゼロトラストの戦略、戦術、姿勢に頼らなければなりません。
- ゼロトラストプログラムを成功させるには、デバイスの安全確保について積極的かつこれまで以上に拡張した考慮が必要です。
- デバイスの安全性確保には、ファームウェアおよびハードウェアレベルの詳細な検知、評価、および修復機能が必要です。

大統領令は、米国国立標準技術研究所（NIST）およびその他の連邦政府の情報源からの標準および文書を読み手に示しています。それらの1つであるNIST SP 800-207は、”ゼロトラスト”を定義し、大統領命令の範囲を理解するための重要なその背景情報も提供します。

“ゼロトラスト（ZT）とは、サイバーセキュリティのパラダイム（在り方）を進化させた言葉で、防御をネットワークベースの静的な境界線から、ユーザー、資産、リソースに焦点を当てたものです。.....”

“ゼロトラストとは、資産やユーザーアカウントの物理的またはネットワーク上の配置（ローカルエリアネットワークとインターネット）や、資産の所有権（企業所有か個人所有か）に基づいて、暗黙の信頼が与えられないことを想定しています。”

“認証と承認（サブジェクトとデバイスの両方）は、企業リソースへのセッションが確立される前に実行される個別の機能です。”

NISTの特別刊行物によれば、“ゼロトラストは、ネットワークセグメントではなく、リソース（資産、サービス、ワークフロー、ネットワークアカウントなど）の保護に焦点を当てており、ネットワークのロケーションがリソースのセキュリティ上の要件として主要な構成要素とは見なされなくなっています”と定義されています。

この定義は、サイバーセキュリティの戦略担当者、実装担当者、実務担当者に、現代のネットワーク上のエンドポイント、サーバー、デバイスに対して業界がこれまでに定義していた、固有の、暗黙の、そして日々低下してしまう信頼を再考することを促します。

セクション3：ゼロトラストとデバイス

上記のNISTの説明からの重要なポイントは、今後のCISOの視点の大幅な変化をもたらします。ゼロトラスト戦略により、サイバーセキュリティチームは“構築”レベルから“アトミック（個々）”レベルに移行する必要があります。例えて言えば、私たちは、より良い、より高い、より強靭な城壁を構築することに囚われてはいけません。その代わりに、城の中にいるすべての人、家、車、ペットのセキュリティ状態を、常に、緊密に、リアルタイムで把握しなければならないのです。この継続的な認識は、ネットワーク内のすべてのエンティティのリスク、脅威、および防御能力を包括して管理する必要があります 。

この大統領令は、設計と実践の両方で“ゼロ・トラスト・アーキテクチャー”を採用することを非常に強く推奨しています。セキュリティ戦略としてのゼロトラストは、理解と確認が必要ないくつかの具体的な概念を前提としています：

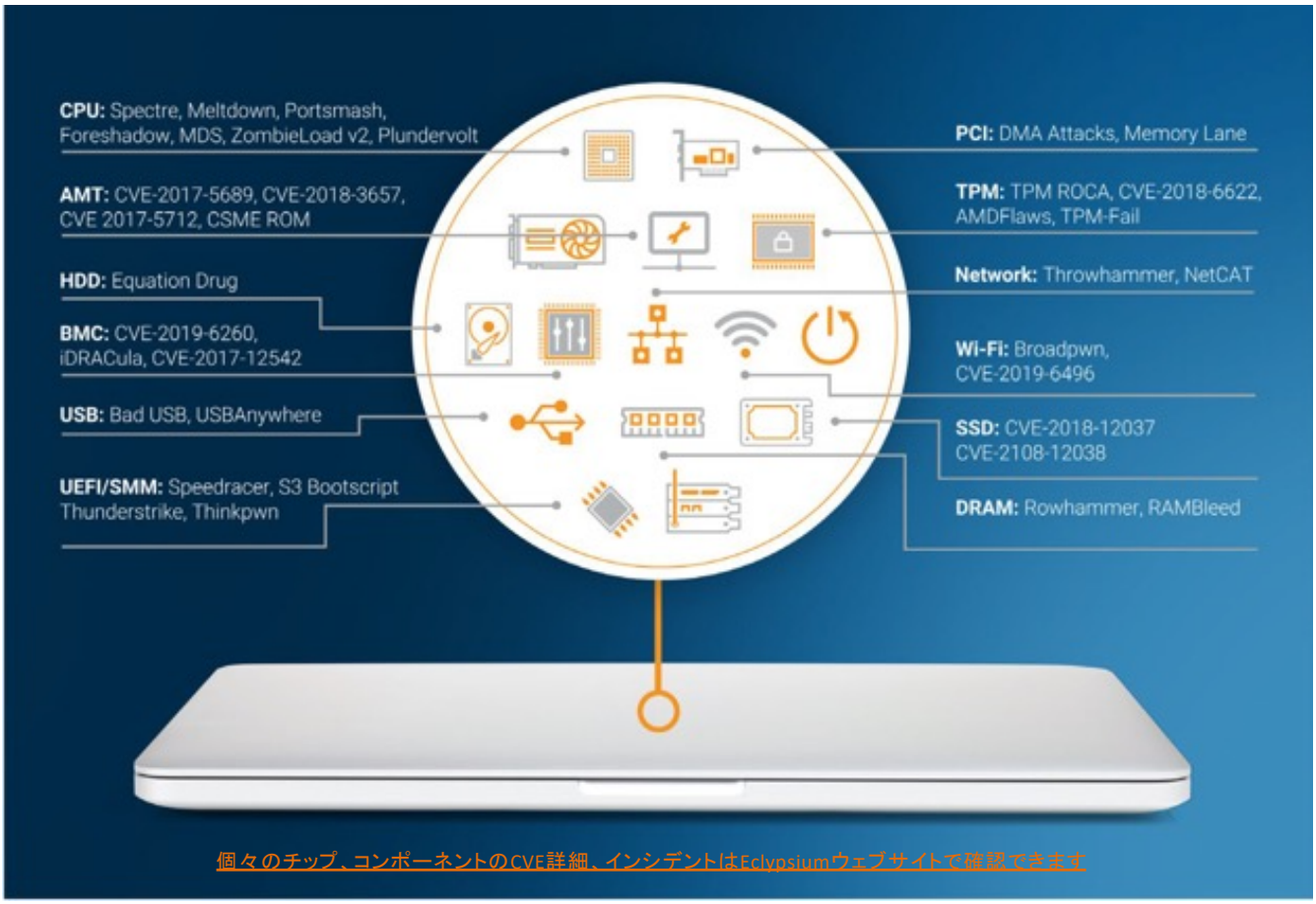
1. **デフォルト拒否**：すべてのデバイスからのすべての新しい接続は、すべてのセッションで正常に認証されるまで、デフォルトで承認されるのではなく、デフォルトで拒否される必要があります。以前のアクセス許可または認証は、以前のセッションから”継承“できなくします。

2. **コンテキスト認証**：その認証は、現時点でそのデバイスとそのユーザーを取り巻くリスク、脅威、またはセキュリティ体制に応じて、本質的にコンテキスト（背景を含む）認証である必要があります。検出されたリスクまたは脆弱性のレベルが変更された場合、昨日付与された認証が今日機能しない可能性があります。

3. **きめ細かい制御**：システムのすべてのエンティティまたはメンバーだけでなく、システム内のすべてのコンポーネントの“デフォルトの拒否”と“コンテキスト認証”。つまり、デバイスのグループ（および人）は、個々のメンバーまたはコンポーネントを一意に認証および承認しない限り、承認できません。これにつきましては、次のセクションで詳しく説明します。

4. **ダイナミック、およびリアルタイム**：ユーザー、ハードウェア、ソフトウェアを問わず、資産とその構成要素の静的な継承リストは、もはや受け入れられません。デジタルトランスフォーメーションのスピードに対応するため、資産、ユーザー、ワークロードを検出するサイバーセキュリティシステムは、高度にダイナミックでリアルタイムなものでなければなりません。例えば、これらのシステムは、現在インベントリにあるすべてのデバイスが明日には交換される可能性があることを想定する必要があります。また、新しいデバイスやデバイスコンポーネントが環境に入ってくると同時に、それらをリアルタイムで検出することができなければなりません。

もちろん、ゼロ・トラスト戦略の策定と実行には、他の要素も必要です。しかし、この4つのポイントは、最初の、そして基本的な理解を得るためのポイントとなるものです。



デバイスの保全評価システムには、ハードウェアおよびファームウェアレベルの脆弱性だけでなく、アノマリや設定ミスの評価を含みます。

セクション3：ファームウェアのコンテキストでのゼロトラスト

前述の4つの原則は、ゼロトラスト戦略をネットワークの目立たない部分、つまりハードウェアとそれに付随するファームウェアにどのように適用する必要があるかを理解するためのフレームワークを提供します。ファームウェアはすべてのコンピューティングデバイスに存在しています。一般的なラップトップコンピューターには、UEFI/BIOSシステムファームウェア、トラステッドプラットフォームモジュール（TPM）、周辺機器、ストレージデバイス、ネットワークインターフェイスカードなど、12を超える内部コンポーネントがあります。各コンポーネント上では、複雑なサプライチェーン内の無数のベンダーによって開発された数百万行のコードを実行します。

1. ファームウェアの“デフォルト拒否”：InfoSecの実践者は、“デフォルト拒否”の概念を認証の問題と考える傾向があり、広義の意味ではそうです。しかし、私たちは、知識、所有、継承といった伝統的な認証要素を用いて、ユーザーやデバイスなどのエンティティを“認証”するという行為を再考する必要があります。認証が“要求者の身元の保証”を意味するのであれば、その要求されたアイデンティティに関連するすべての部分、例えば、ベアメタルハードウェア、そのさまざまなコンポーネント、さらにそれらの配下で動作するファームウェアの実行方法を指示し、基本的な組み込みファームウェアが改ざんされていないことの保証を裏付ける必要も含まれます。“デフォルトの拒否”の原則は、正しく署名または認定されていないファームウェアの実行を許可してはならず、その結果、サービスを提供するデバイスが起動しないようにする必要があることを示しています。

2. ファームウェアの“コンテキスト認証”：”コンテキスト認証”の概念には、ファームウェアに関して独自のアプリケーションがあります。上記の一般的な説明にあるように、”検出されたリスクまたは脆弱性のレベルが変更された場合、昨日付与された認証は今日は機能しない可能性があります”。ファームウェア中心の例では、デバイスが接続を試み、デバイスに脆弱性または構成ミスが最近示されたファームウェアバージョンが含まれている場合、この認証要求は拒否する必要があります。この種のファームウェアの脆弱性の最近の例は、CVE-2019-3707にあります。ここでは、Dellシステムをサポートするファームウェ

アと、Dell独自のリモートアクセス機能を使用する機能に複数の脆弱性が発見されました。デバイスのコンテキスト認証の実践は、影響を受けるファームウェアバージョンの1つを含むDellデバイスは、前日にアクセスが許可されていたとしても、ネットワークへのアクセスを拒否する必要があることを示唆しています。

3. ファームウェアに関連する”きめ細かな管理”: ”すべてのデバイスにファームウェアがある”ことを単に認めるだけではもはや十分ではありません。実際、ほぼすべてのコンピューターに見られるユビキタスなUEFI(Unified Extensible Firmware Interface)をはじめ、オンボードメモリ、ネットワークコンポーネントからビデオドライバーまで、すべてのデバイスのすべてのコンポーネントに独自のファームウェアがあります。ファームウェアインスタンスは現在、多数の統合コンテナ内にネストされており、エンドポイントとサーバーが数十のファームウェアファイルでサービスを開始することは珍しくありません。

4. ファームウェアのコンテキストでの”ダイナミックかつリアルタイム”: ハードウェアの作成、配置、保守、交換は、定期的に行うのではなく、継続的に行うように進化し、現在ではリアルタイムで行われています。仮想サーバーは、数千の単位で、しかも一瞬のうちに交換されたり停止したりします。これにはファームウェアが含まれます。すべての家庭のすべてのデバイス、およびビジネスネットワーク内のすべての隣接するデバイスはダイナミックに変更され、一時的なものである可能性もあり、絶えず変化する可能性があります。これには、関連するファームウェアの数百万行が含まれます。導入初期に作成された管理表、またはまれなインベントリアップデートでは、これらのデバイスの整合性を保護および保証できません。

ファームウェアとそれらがサポートするデバイスは、すべてのコンピューティングおよびネットワーキングシステムの基盤の構成要素であるだけでなく、ゼロトラスト戦略を作成および実行するための重要な要素です。

セクション4：サプライチェーンのファームウェア

大統領令のセクション4の大部分は、”主要なソフトウェア”にソフトウェア部品表（SBOM）を添付して、意図した整合性を維持する必要があるという要件の定義が記述されています。

> ”…正確で最新のデータ、ソフトウェアコードまたはコンポーネントの確証（つまり、出所）を維持し、ソフトウェア開発プロセスに存在する内部およびサードパーティのソフトウェアコンポーネント、ツール、およびサービスを管理し、監査を実行する。そして、これらの管理を定期的に実施します。“

これは、エンドポイント、サーバー、IoTデバイス、およびネットワークデバイスに組み込まれているファームウェアでは特に難しいことが証明されています。 2019年に公開されたSupermicroサーバーファームウェアの脆弱性の場合のように、クラウドサービスをサポートしているように見える十分に保護されたシステムでも、これは難しい作業です。

最新のテクノロジーサプライチェーンの複雑さは、多くのリスクに晒される可能性をもたらします。デバイスOEMは、他のサプライヤから基盤となるコンポーネントを調達することが多いコンポーネントサプライヤのネットワークに依存しています。ほとんどの場合、これらのデバイスにはそれぞれ付属のファームウェアが必要となります。サプライチェーンのこれらのポイントのいずれかで妥協すると、デバイスの整合性が危険にさらされる可能性があります。コンポーネントの脆弱性により、悪意のある攻撃者が、製造プロセス中、付加価値再販業者（VAR）内、またはファームウェア更新プロセス中に、サプライチェーンの工程後半でデバイスを改ざんする可能性があります。

デバイスの出所、履歴 ー 真正性や品質の目安となるデバイスの所有者の記録 ー は、多くの場合、他の種類のソフトウェアやハードウェアよりも、ファームウェアの方が厄介な問題です。システムコンポーネントは価格に基づいて選択されることが多く、上流の取引や改訂された契約に基づいて変更できます。それらのライブラリとファームウェアの詳細は、最終的にシステムのセキュリティ保護を担当するエンタープライズセキュリティチームには表示されないことがよくあります。

これらの課題にもかかわらず、大統領令はサイバーセキュリティチームにすぐに以下の2つのことをするように求めています：

1. 完全なSBOMの必要性をベンダーに伝える
2. デバイスの管理者が公開されたSBOMを活用して、取得および展開プロセス全体で機器を検証できるようにする

これらのアクションの両方にファームウェアの完全な評価を含める必要があるというのが私たちのスタンスです。

セクション4：すべてのファームウェアが”重要なソフトウェア”である理由

大統領令は”重要なソフトウェア”の概念に細かい部分まで記述しています。

”「重要なソフトウェア」 ― 重要なソフトウェアとは、信頼に関わる機能を果たすソフトウェア（例えば、昇格したシステム権限を与えたり、ネットワークやコンピューティングリソースへの直接アクセスを要求するなど）―の安全性と完全性は特に懸念されます。“

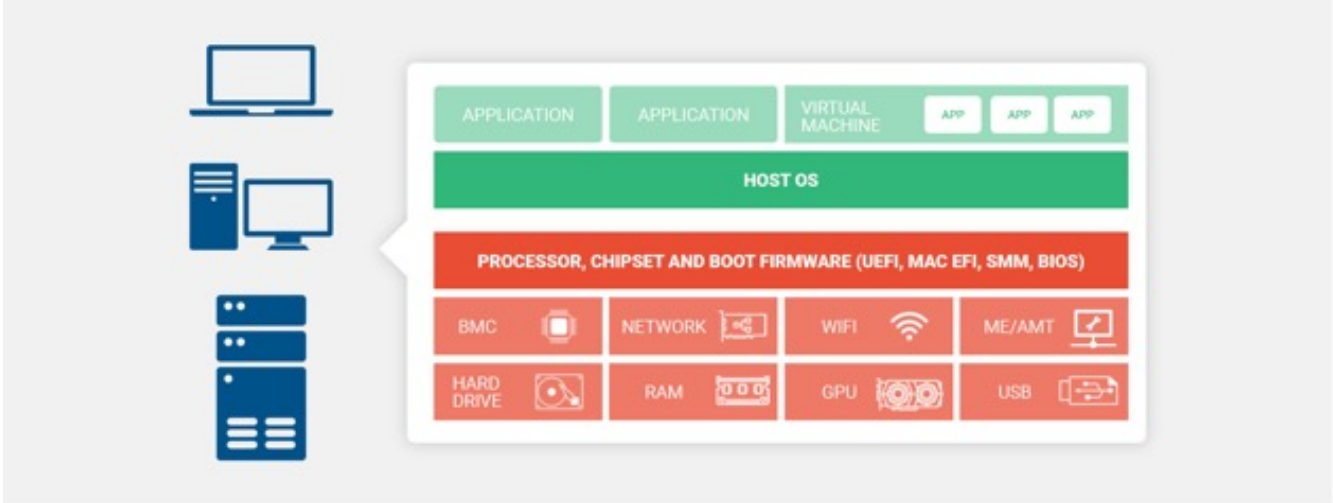
大統領令の基準を見てみると、ファームウェアはその定義を満たしているだけでなく、見落とされたり、監査が不十分であったりすることが明らかになります。大統領令に記載されている重要なソフトウェアの要件は、現代のインフラにおいてファームウェアが果たす役割に直結しています:

- ”機能するために必要な特権のレベル”: ファームウェアは、オペレーティングシステムの下のセキュリティ層（”Sub-Zero”セキュリティ・リング）を占有するため、最終的な特権を持つ場合が多いです。
- ”他のソフトウェアとの統合性と依存性”: ファームウェアは、その性質上、オペレーティングシステム、アプリケーション、およびサービスが統合され、依存する最初の機能的な構成要素です。
- ”ネットワークおよびコンピューティングリソースへの直接アクセス”: 定義的には、ファームウェアは、その性質上、ほぼすべてのネットワークやコンピューティングリソースの「中、もしくは上に」あるものであり、最も直接的なアクセスを実行しています。
- ”信頼に不可欠な機能を提供”: 信頼されたプラットフォームモジュールからあらゆる種類のブートプロセスまで、信頼されるインフラストラクチャの最も重要な構成要素の一部は、ファームウェアに完全に依存しています。
- ”侵害された場合の被害の可能性”: システムに被害を与える方法として、ファームウェアの侵害よりも効率的で持続性のある方法はないかもしれません。LoJaxやTrickBootといった悪意のあるコードによる攻撃や、Supermicro社のサーバに対する攻撃で見られたようなBMC（Baseboard Management Controller）への攻撃は、サイバーディフェンダーが経験した最大の被害を受けた攻撃と言えるでしょう。さらに、ファームウェアへの攻撃は持続性が高く、システムを消去してベアメタル構成に復元した後も続くことが知られています 。

オペレーティングシステムの”下”にあるコード、マイクロコード、および組み込みファームウェアの量は増加しているだけでなく、頻繁に攻撃者の標的となっています。

最終的に、ファームウェアの侵害は、システムの機密性を無効にし、整合性を破壊し、システムとサービスの可用性を妨げる可能性があります。データの損失とコンピューティングデバイスの破壊に加えて、変更されたファームウェアは、データの透過的な変更を可能にし、他のセキュリティ制御を覆すことで、信頼できる計算が完全に欠如することになります。これらの点を念頭に置くと、すべてのファームウェアが実際に重要なソフトウェアであるという概念に異議を唱える人はいません。

ガートナーは、2020年のレポート”エンドポイントセキュリティを改善するためのロードマップ”で、”スクリプトコントロールが厳しくなるにつれて、ファームウェアが高度な攻撃者の次のエンドポイントの戦いの場になる可能性がある”と述べ、この議論に警鐘を鳴らしてます。



オペレーティングシステムの”下”にあるコード、マイクロコード、組み込みファームウェアの量は増加しているだけでなく、攻撃者に狙われる頻度も高くなっています。

デバイスのインティグリティ管理（保全）を”ゼロトラスト”と”クリティカルソフトウェア”の両方にどのように適応するか

”インテグリティ”は、具体的で狭い解釈と、刺激的で示唆に富む解釈の両方を備えた便利な言葉です。インテグリティとは、次のことを意味します。

- 完全または未分割の状態、または品質：完全性
- 障害のない状態：健全性
- 特に道徳的または芸術的価値観の規範をしっかりと順守する：不朽性

”デバイスのインテグリティ”とは、デバイスとその基盤となるファームウェアの完全性、健全性、および不朽性を保証することです。

- 完全性：ファームウェアはデバイスに完全で最新のものを使用していますか？現在監視されているファームウェアバージョンにパッチを適用または更新するために、別のバージョンが導入されていますか？
- 健全性：このバージョンのファームウェアに対する既知の脆弱性またはアクティブなエクスプロイトはありますか？これらの脆弱性にどのように優先順位を付けたり、軽減対策したりしていますか？
- 不朽性：デバイスの整合性は、ファームウェアが現在の使用法と状況に対して可能な限り安全になるように構成および配置されていますか？

デバイスインテグリティの実践は、エンドポイント、モバイル、IoT、ネットワークデバイスなど、ネットワーク上のすべてのデバイスに関するこれらの事項を確認します。すべてのデバイスの動作は、命令を与えるDNAとして機能するファームウェアによって制御されるため、まずこれらの質問を基盤となるファームウェアに適用しますが、該当する場合は、ベアハードウェアにも適用します。

ゼロトラストの世界では、ネットワークに参加するすべてのデバイスについて、これらの各属性（完全性、健全性、および不朽性）を確認します。これらのいずれかでチェックをおろそかにすると、そのデバイスがネットワークに参加してその組織のビジネスを推進するために十分であると組織が判断するデバイスインテグリティの信頼性が低下し始めます。

また、このファームウェアのレビューは、実際に”重要なソフトウェア”と見なされるものの一部であると想定して開始します。非常に特権があり、ソフトウェアの他の部分と統合されており、基盤となるハードウェアに直接アクセスできます。”信頼”の概念にとって重要であり、侵害された場合重大な問題が発生する可能性が非常に高くなる可能性があります。

デバイスの整合性、およびそれが尋ねる質問とそれが提供する回答は、デバイスの最も隠された部分、ひいてはデバイス自体の整合性を保護および保証するために必要なツールを提供します。。

デバイス・インテグリティにはリアルタイムでの脅威の把握が必要

ファームウェアイメージまたは埋め込まれたマイクロコードの詳細な評価と評価によって、デバイスの完全性、健全性、および不朽性を保証することは、デバイスの全体的な整合性を保証するための重要なステップです。しかし、新しい攻撃のスピードが速く、動的な性質を持っているため、デバイスとそのファームウェアの完全性、健全性、および不朽性は、現在の脅威と悪用の積極的な分析と組み合わせる必要があります。

2021年に開催されたRSAカンファレンスで、Guardicore社の研究者であるOfri ZivとJJ Lehmanは、直観的、かつどこにでも起きえるファームウェアレベルのインプラントをデモしました。セッションでは、“WarezTheRemote? Under the Couch, and Listening to you,(ソファの下であなたの話に聞き耳立てています)”というセッションで、2人は、現代のほぼすべての家庭に存在するファームウェアに存在する未知の脆弱性を利用して、プライバシーを侵害するような操作を行うことができることを示しました。

デモで使用されたのは、米国で広く使われ利用者は1000万人を超えるいると言われるComcastのセットトップボックス「Xfinity X1」用のリモコンでした。このリモコンは、音声コマンド対応のため、マイクロフォンと、かなり高性能なプロセッサーを搭載しています。このリモコンに悪意のあるファームウェアの埋め込みによって数分のうちに最小限の費用で、ハッキングしユーザーの操作なしで継続的かつリモートで音声を録音しました。

この単純なファームウェアレベルのハッキングは、急速に変化する新しいデバイスレベルの脆弱性の氾濫によって、今後12か月で脅威の状況を大きく変える可能性があることを示唆しています。しかしながら、エンタープライズセキュリティチームは、”Comcastのリモコンが手元にないのに、なぜ気にするのか”と疑問視する場合があります。

その答えは、このセッションで、会議電話、ビデオ機器、VPNシステムなど、他の企業内ネットワーク機器の脆弱性を、簡単かつ安価に突く方法を明らかにしたことにあるのではないでしょうか？また、このセッションでは、私たちの最も一般的なデバイスが、気にもされず、テストされず、保護されていない状況であることにも言及しました。

デバイスインテグリティの3つの柱

デバイスインテグリティの問題が、既存の脆弱性管理、パッチ管理、または脅威検出製品では解決できない理由を確認してみましょう。至極単純な回答としては、これらの製品はその目的のために作られていないので、解決できないということです。これらの製品は、ファームウェアレベルおよびデバイスレベルの侵害の脅威が現実のものとなり、蔓延する前に、主に設計および展開されました。率直に言えば、これらの製品は、この最新世代の脅威とエクスプロイトのファームウェアレベルの深刻な脅威への対策のために作成されたものではありません。

デバイスインテグリティの問題に対するエンタープライズクラスのソリューションは、速度と規模で機能するIDENTIFY（識別）、VERIFY（検証）、およびFORTIFY（防御）の3つの方式を通じてこれらの問題に対処します。

IDENTIFY（識別）: このソリューションは、企業や公共のネットワーク全体で、デバイス、サーバー、エンドポイントを発見することができます。このソリューションは、デジタル環境全体を完全に把握することも、特定のデバイスグループに焦点を当てて把握することも可能で、組織のセキュリティ体制を決定するファームウェアやコンポーネントを常に把握することができます。また、エージェントベースとエージェントレスの技術を適切に組み合わせて、新たに導入されたデバイスをリアルタイムで検出します。この識別には、ハードウェアインプラント、バックドア、その他の悪意のあるコードなどの脅威を警告する高度な脅威検知機能が含まれます。

VERIFY（検証）: このソリューションは、信頼されたベースラインに対してデバイスを検証します。このデータを、業界最大のグローバルなファームウェア・レピュテーション・データベースと比較し、数百万のファームウェア・ハッシュと数十のエンタープライズ・ハードウェア・ベンダーとの間で、ファームウェアのアイデンティティをチェックし、ベースラインの変更を特定します。そして、古いファームウェアを発見し、改ざんを明らかにします。また、デバイス内の弱点や脅威を把握し、ハードウェアプロファイルの変更、改ざん、危殆化に関連するリスクを検出することができます。エージェントベースおよびエージェントレスのスキャニングにより、あらゆる種類のデバイスにおけるファームウェアの脆弱性や保護機能の欠落を検出することができます。

FORTIFY（防御）: 誤設定、脆弱性、または脅威が発見された場合、このソリューションはパッチ適用や更新作業を加速させ、スタッフが弱点に対処して時間を節約することを可能にします。また、脅威が発生した場合には、堅牢なAPIを使用して、アップデートの適用や影響を受けたデバイスの隔離などの自動化されたオーケストレーションアクションを実行することで、被害を防ぐことができます。さらに、デバイスの分析とフォレンジック機能により、デジタルフォレンジックが証拠を収集し、攻撃の背景を調査したり、侵害を特定してその範囲を限定したり、インシデント対応のプレイブックを完成させることができます。

今日できること

国家のサイバーセキュリティの向上に関する大統領令は、新しいレベルのセキュリティと回復力を実現するための、長いがアクセス可能な道のりを示しています。また、重要なシステムとデータのセキュリティにおけるデバイスとファームウェアの役割を新たに理解した上で、今日の新しい要件に対応するための「1、2、3」の道筋を示しています。

これらのステップの中で:

1. ゼロトラスト戦略、戦術、姿勢の採用
2. ゼロトラストプログラムの成功のための、ファームウェアレベルの脆弱性、脅威、リスクに焦点を当てた、アクティブで拡張されたデバイスインテグリティの理解の確立
3. 大規模な企業でデバイスの完全性を実現するためには、IDENTIFY（識別）、VERIFY（検証）、FORTIFY（防御）という方式で、ファームウェアおよびハードウェアレベルの詳細な発見、評価、修復機能の導入が必要

Eclypsiumプラットフォームは、ラップトップ、サーバー、スイッチ、ルーター、その他のシステムなど、組織の重要なデバイスを継続的に保護するエンタープライズクラスのソリューションです。このプラットフォームは、Linux、Windows、MacOS、Cisco-IOSなどの幅広いオペレーティングシステムをサポートしています。

すべてのデバイスには、ファームウェアが存在し、独自の脆弱性と脅威モデルを持つ多数のコンポーネントがあるため、Eclypsiumは、システムUEFIとBIOS、プロセッサとチップセット、トラステッドプラットフォームモジュール、インテルマネジメントエンジン、PCIデバイス、サーバーBMC、ブートローダー、ネットワークコンポーネントを含むすべての拡張コンポーネントで同じ可視性とセキュリティを提供します。Microsoft SCCM、Intune、Taniumなどのツールと統合し、一般的なSSOプロバイダーとのアクセス管理もサポートします。

SplunkやQ-Radarなどの主要なSIEMソリューションのユーザーは、デバイスレベルおよびイベントデータをインポートして可視化し、動的分析を実行できます。Eclypsiumプラットフォームは、他の既存のセキュリティソリューションに統合するための豊富なREST-APIセットも提供します。

ファームウェアリスク、デバイスインテグリティ、またはEclypsiumプラットフォームの詳細についてご興味のある方は、jp-info@eclypsium.comにご連絡ください。