製品概要

ネットワークデバイスへのエクリプシウム

概　説

VPN、スイッチ、ファイアウォール、ルーター、およびさまざまなコンセントレーター、ゲートウェイ、コントローラーなどの企業向けネットワーク機器は、ランサムウェアのトップファミリーや国家レベルの脅威の標的となってきています。しかし、従来のサーバやラップトップとは異なり、ネットワーク機器はほとんど更新されません。さらに、従来のセキュリティエージェントでは保護することができず、単純な脆弱性スキャンでは見逃されてしまうような脆弱性が、基本的なデバイスコードやファームウェアに含まれていることがよくあります。

Eclypsiumファームウェアセキュリティプラットフォームは、この重要なレイヤーにシンプルで自動化されたセキュリティをもたらし、企業はネットワークデバイス内のソフトウェア、ファームウェア、ハードウェア、コンポーネントを簡単に識別し、検証し、強化することができます。これにより、企業はネットワーク機器内のソフトウェア、ファームウェア、ハードウェア、コンポーネントの識別、検証、強化を容易に行うことができます。セキュリティチームは、機器の発見、脆弱性の評価、パッチの適用、脅威の検知と対応、サプライチェーンのリスク管理など、ネットワーク機器のファームウェア層に至るまでのセキュリティを簡単に自動化できる単一のツールを入手可能となりました。

ファームウェアへの攻撃の現状

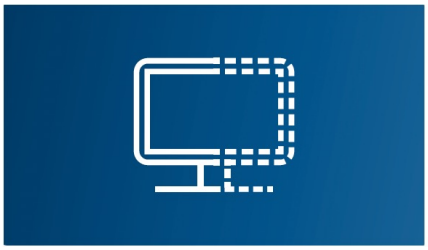
2019年後半から、米国のセキュリティ機関であるCISAは、PulseSecure、Cisco、Citrix、F5、Fortinet、Juniperなどのエンタープライズベンダーが提供する多種多様なネットワークデバイスを標的とした、ロシア、中国、イランを発端とする国家的な攻撃を詳細に説明する一連のアラートに関するレポートを発行しました。攻撃者は、これらの機器の脆弱性を一貫して利用し、環境への最初のアクセスを得て、追加のマルウェア・ペイロードを拡散することができました。これらの手法は、その後、REvil、Ryuk、Conti、さらにNetwalkerなどの使用頻度の高いランサムウェアに使用され、最終的に数百社の企業に影響を与えました。

コアとなる機能

ネットワーク機器向けエクリプシウムソリューションは、クラウド型のファームウェアセキュリティソリューションで、デバイスにエージェントをインストールすることなく、ネットワークデバイスやネットワークインフラを完全に可視化し、制御することができます。主な機能としては、以下のようなものがあります：

認識

ネットワークデバイスの自動検出、ファームウェア、ハードウェア構成、ネットワークデバイス内の数十個のコンポーネントの継続的な可視化を提供します。セキュリティに影響を与える可能性のある重要なデバイス、コンポーネント、属性、または変更点を迅速に把握することができます。



検証

すべてのファームウェアのインティグリティを検証し、ルートキット、インプラント、バックドアを含む既知および未知のファームウェアの脅威を検出します。古くて脆弱なファームウェアやデバイスの誤設定によるリスクを積極的に特定します。

強化

パッチやアップデートをリモートで適用し、デバイスのリスクを積極的に軽減します。ファームウェアに変更があった場合、自動でアラートを受信し、既存のITツールやセキュリティツールとの統合により、自動で対応することができます（主要なSIEM、脆弱性管理ツール、デバイス管理ツールとの統合確認済み）。

具体的使用例の紹介

ランサムウェアと高度な脅威からの保護

ランサムウェアに積極的に悪用されている脆弱性を持つネットワーク機器を積極的に特定する。ファームウェアに特化したランサムウェアやマルウェアを検知します。デバイスにファームウェアのインプラントやバックドアが存在しないことを確認します。ファームウェアのインティグリティが変更された場合、自動的にアラートを受け取ることができます。

ネットワークデバイスのエージェントレスな発見と分析

Eclypsiumのエージェントレスソリューションは、マネージドエンドポイントを使用して、企業環境内のネットワークデバイスを自動的に検出します。このユニークな分散型アプローチにより、セキュリティチームはネットワークデバイスにセキュリティエージェントをインストールする必要がなく、追加のコードを追加したり、変更ウィンドウを待ったりすることなく、簡単にデバイスにセキュリティの可視性を得ることができます。

リスク評価と改善

デバイスを危険にさらす可能性のある脆弱性や設定ミスのあるネットワークデバイスを自動的に特定し、実際の攻撃で狙われている脆弱性を優先的に特定します。デバイスのインティグリティを検証し、既知および未知の脅威を検出します。古くなったデバイスや脆弱性のあるデバイスのファームウェアをリモートでパッチやアップデートすることで、デバイスを安全な状態に保ちます。ファームウェアの更新方法は、ベンダーによって異なります。

サプライチェーン・リスクマネジメント

購入前に機器ベンダーやサービスプロバイダーを評価し、脆弱性や安全でないコンポーネントや構成を特定します。新たに取得したシステムを検証し、サプライチェーン上で侵害されていないことを確認するとともに、脆弱性やSBOMへの予期せぬ変更を積極的に特定します。

詳細な機能と特徴

認識：デバイスの発見とインベントリ

Eclypsiumは、企業環境にあるネットワークデバイスを自動的に発見し、識別します。このプラットフォームは、ネットワーク機器のコンポーネントや構成を含む詳細な情報を収集し、分析します。可視性のオプションはベンダーによって異なりますが、以下のような詳細情報が含まれます：

- **基本的な識別情報** - IPアドレス（オプション）、MACアドレス、ホスト名、オペレーティングシステム（ベンダー、バージョンなど）などのデバイスの特徴
- **ファームウェアおよびハードウェアの詳細情報** - プロセッサ、チップセット、デバイス、ファームウェアベンダー、リリース日、システムおよびデバイスのメーカー、モデル番号など
- **ハードウェアの状態および構成** - PCI/PCIe情報、ブートローダー、ハードウェアおよびファームウェアの構成、ベンダー固有のファームウェア、およびその他のタイプのファームウェア

検証：脆弱性評価とパッチ適用

Eclypsiumは、すべてのファームウェアとデバイスの設定を分析し、デバイスのセキュリティ姿勢に影響を与える問題を検出します。これにより、リスクに基づいてデバイスを識別・調査し、利用可能なアップデートを適用してリスクを修正することが容易になります。主な機能は以下の通りです：

- **古いファームウェアの検索** - 脆弱性やその他のデバイスの問題を含む可能性のある古いファームウェアを持つデバイスを検索します
- **脆弱性の発見** - 従来のソフトウェアによる脆弱性スキャンでは見逃されがちな、システムやコンポーネントのファームウェアに影響を与える脆弱性やCVEを持つデバイスを特定します
- **デバイスをリスクでソート** - 累積リスクに基づいてデバイスを素早くソートします。OS、グループ、ベンダー、製品、コンポーネント、セキュリティ機能、脆弱性などでフィルタリングすることで、さらに詳細な表示が可能です
- **脆弱性による検索** - 特定の脆弱性を検索して調査し、影響を受け、特定の脆弱性に対してスキャンされたすべてのデバイスを見つけることができます

検証 : 脅威の検知と対応

Eclypsiumは、アクティブな脅威の兆候がないかデバイスを分析します。これには、既知および未知の脅威の検知に加え、デバイスのインティグリティに対する予期せぬ変化を特定するための継続的な監視が含まれます。

- **デバイスベースラインの変更** - ベースラインに変更が加えられたデバイスを迅速に特定し、重要性の高いシステムに予期せぬ、あるいは計画外の変更が加えられた場合、それを容易に認識することができます
- **未知のバイナリの検出** - Eclypsiumは、業界で最も広範な既知のベンダーのファームウェアのライブラリを維持しており、この継続的にメンテナンスされるホワイトリストに載っていないファームウェアを識別することができます
- **既知の脅威の検出** - ルートキット、ハードウェアインプラント、バックドアなど、さまざまな既知の脅威の存在を検出します。また、ユーザーは独自のファームウェア固有のYARAルールをインポートし、定義することができます
- **異常な動作** -ファームウェアの動作は通常においては予測可能です。これにより、Eclypsiumはファームウェアを分析して、潜在的な脅威を示唆する異常な動作や機能を明らかにすることができます

強化 : パッチ適用と自動応答

Eclypsiumは、プロアクティブに問題を解決し、ファームウェアのリスクを軽減するためのツールをチームに提供します。セキュリティチームは、脆弱性を修正するためにファームウェアやデバイスコードを簡単に更新し、セキュリティイベントに対応するために自動化されたアラートやワークフローを起動することができます。

- **パッチマネジメントとアップデート*** - Eclypsiumコンソールを介して直接デバイスの問題を修復したり、APIを介してファームウェアアップデートをダウンロードしてインストールします
- **自動応答** - 強力なREST APIは、SIEMやSOARソリューションなどの他の企業のセキュリティツールと統合し、自動応答やプレイブックを起動します
- **ダイナミックアラート** - 設定可能なアラートにより、特定の脆弱性や侵害の兆候がないかデバイスのグループを監視し、それらが検出されたときにエンドポイント運用チームやインシデント対応チームに通知することができます

*2021年8月現在はCisco社製デバイスに限定されます

ネットワークデバイスのためのEclypsium：対応デバイス

Eclypsiumは、Arista、Cisco、Citrix、F5、Fortinet、Juniper、Palo Alto Networks、Pulse Secureなどの幅広いネットワークデバイスベンダーに対応しています。

インテグレーション

Eclypsiumプラットフォームは一般的なデプロイメントツールやセキュリティツールと統合されており、企業のデバイスをファームウェアやハードウェアレベルまで簡単に管理・保護することができます。強力なREST APIにより、企業はEclypsiumを既存のツールやプロセスと統合することができます。検証済みの統合機能は以下の通りです：

Eclypsiumのデプロイメント		可視性の向上と分析
• Airwatch by VMWare • JAMF • Microsoft Intune	• Microsoft SCCM • Tanium	• Intel intelligence feeds

システムへのアクセスと認証		セキュリティ・アナリティクス
• Cloudflare Access • Okta	• Ping Identity • Google OSS	• Kenna Security • Splunk

Eclypsiumについて

Eclypsiumは、企業向けのファームウェアセキュリティ企業です。当社の包括的なクラウドベースのプラットフォームは、ラップトップ、タブレット、サーバ、ネットワーク機器、コネクテッドデバイスなど、お客様の広範なグローバルネットワークに存在するあらゆる場所で、ファームウェアとハードウェアを識別、検証、強化します。Eclypsiumのプラットフォームは、持続的かつ密かなファームウェア攻撃からの保護、継続的なデバイスのインティグリティの提供、大規模なファームウェアパッチの提供、ランサムウェアや悪意のあるインプラントの防止を行います。セキュリティ意識の高いフォーチュン1000企業や連邦政府機関に支持されているEclypsiumは、Gartner社の「Cool Vendor in Security Operations and Threat Intelligence」、TAG Cyber社の「Distinguished Vendor」、Fast Company社の「World's 10 Most Innovative Security Companies」の1社として選ばれています。
Eclypsiumに関するお問い合わせは jp-info@Eclypsium.com へ日本語でお気軽にお問い合わせください。