Vdoo securing the connected everything

ルーターのセキュリティ強化に Vdoo を選んだ ネットワーク機器ベンダーの ケーススタディ

japan_info@vdoo.com

https://www.vdoo.jp

一般向け

備考: このドキュメントには、ネットワークルーター製品のセキュリティに Vdoo を利用している大手ネットワーク機器ベンダーのプロジェクトに関する情報が記載されています。お客様からのご希望により、社名は公開されておりません。

ニーズ

品質とパフォーマンスで評判のネットワークルーターを扱っているこのベンダーは、国際市場における優勢を保つため、デバイスのセキュリティレベルを強化する必要性を認識しました。

VPNFilter や Mirai をはじめとする、ルーターを含むネットワークデバイスを標的としたサイバー攻撃により、近年セキュアなネットワークデバイスを求める声が急速に高まっています。これらの攻撃は Linux を実行しているルーターを標的にし、ネットワーク機能に完全なシャットダウンを含む重大な影響を与えました。

同社は顧客や長年にわたるインテグレーションパートナー、規制機関、標準化団体からのサイバーセキュリティに対する要求の増加を考慮し、自社のデバイスセキュリティとプロセスを強化することを決めました。同社はこの目標に向け、主力ネットワークルーターモデルの最新バージョンのセキュリティ強化という、ハイインパクトのプロジェクトに着手しました。

お客様の情報

- 大手グローバルベンダー
- 本社: 北米
- 通信、防衛、製造、放送など、さまざまな業界の顧客と取引
- 行政機関や大企業向けのネットワークルーターの大手プロバイダー
- 顧客や規制機関からのサイバーセキュリティに関する要求が増加

同社では、このプロジェクトで導入されるメソドやテクノロジーがこのモデルのルーターのセキュリティ強化という直接の成果に加え、将来の製品バージョンやモデルの早期開発段階におけるセキュリティ慣行の改善にも役立つと考えていました。

課題

当時開発チームは、自社のセキュリティに関するニーズに合わせて社内でカスタマイズされたオープンソースのコードスキャンツールを使用し、一人の開発者が製品セキュリティチームと協力し、スキャン結果に優先順位を付けていました。しかし、このコードスキャンツールはスキャン結果の項目が非常に多く、担当の開発者は評価と優先順位付けに苦労していました。さらに、同開発者は発見されたセキュリティ問題の解決方法の判断が困難であるとも感じていました。

このコードスキャンツールにはさまざまなセキュリティ問題やバグに対するスキャン機能が搭載されていましたが、実際にデバイスにセキュリティギャップが生じている項目の特定には役立たず、実際の攻撃でどのように悪用されるのかに関するコンテキストも提供されませんでした。

検討されたソリューション

このベンダーでは当初、セキュリティに対する次の 2 つのアプローチが検討されました。

1. **既存のコードスキャンツールの強化** – 社内のセキュリティ専門家がツールをカスタマイズすることで、デバイスに新たな高度な攻撃へのリスクが生まれる可能性があるセキュリティギャップを検出するという方法です。このアプローチでは、一人の人間が潜在的なセキュリティの弱点や脅威への対応範囲を広げ、検出された問題を評価し優先順位を付け、長期的にツールを維持していかなければならないため、当然限界がありました。

2. **アウトソーシングの侵入テストサービス** – 他社にセキュリティチェックを依頼するという方法です。このアプローチの主な欠点は、プロジェクトの期間でした。手動での侵入テストには業者のチームのスケジュールや制約によって、製品またはバージョンごとに長くて数週間かかることもあり、デバイスの販売開始に遅れが出る可能性がありました。また、このアプローチには非常に多くのリソースが必要となるため、多数製品へのスケールアップや製品ごとの繰り返しのセキュリティ検証が不可能でした。

これらの懸念に加え、どちらのアプローチも、テスト結果の取得後のセキュリティギャップの優先順位付けや対策方法の決定に、社内での多大な労力が必要となります。

同社はどちらのアプローチにも大きな欠点があるという結論に達し、他の選択肢を検討し始めた過程で、Vdoo に注目しました。

採用されたソリューション：Vdoo プラットフォーム

最終的にこのベンダーでは、自社のルーター製品のセキュリティ評価と強化に、Vdoo デバイスセキュリティプラットフォームが選ばれました。その主な理由は次の通りです。

- **幅広い対応範囲** – Vdoo のセキュリティチームにより継続的に更新されている豊富なデバイスセキュリティ知識ベースに基づき、既知の脆弱性 (CVE)、セキュリティの不正行為、構成の問題など、幅広いセキュリティ問題を自動的に検出します。

- **スピード** – Vdoo プラットフォームは自動セキュリティ分析ソリューションであるため、手動による侵入テストサービスと比較して大幅な速度の向上を実現し、数週間ではなく数分で結果を提供します。これは、同社が市場投入を遅らせることなく新しいリリースのセキュリティ検証を継続的に行えるよう、今後の継続的な製品開発の取り組みの一環としてセキュリティを導入するプロセスを確立したいと考えていたため、特に重要な要素となりました。

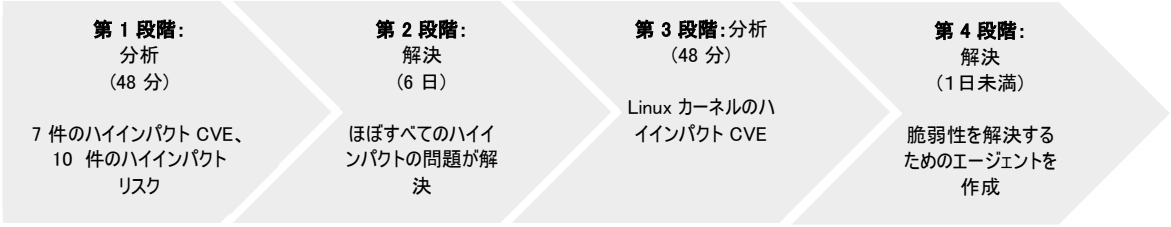
- **効率性とスマートな優先順位付け** – 検出された個々のセキュリティ問題に対し、インテリジェントなインパクトスコアと明確な解決ガイダンスが提供されるため、重大な問題の迅速かつ効率的な優先順位付けと、それらへの対処方法の決定が可能になります。しかもその過程で、社内のセキュリティ専門家が必要となりません。

セキュリティ導入プロセス

このベンダーは、セキュリティの分析と問題の解決を繰り返す包括的なセキュリティの導入を選びました。

同社が決めたプロジェクトの目標は、ルーターに十分なセキュリティレベルに到達させることでした。この目標を果たすには、ハイインパクトのセキュリティ問題を未解決のままにすることはできません。未解決の問題の発見とそれらによるインパクトの評価は Vdoo Vision によって、次のように行われました。

下の図は大まかな流れを示したものです。



Vdoo Vision によるセキュリティ分析とギャップ解決

最初のステップは、デバイスのバイナリーイメージを Vdoo Vision にアップロードすることでした。Vdoo Vision は接続型デバイスのセキュリティ分析を自動的に行うウェブベースのプラットフォームです。Vision は 1 時間足らずでデバイスのソフトウェアコンポーネント（SBOM）の詳細情報、検出されたセキュリティの脆弱性とリスク、解決に向けたガイダンスを提供しました。

初回の分析では 7 件の CVE と 10 件のセキュリティリスクを含む、インパクトスコアが高い（または非常に高い）セキュリティ問題が 17 件検出されました。例：

- **リスク 1:** SSL 通信に脆弱な暗号キーが使用され、総当たり攻撃のリスクにさらされていました。
  解決ガイダンス: 使用されているアルゴリズムに適切な NIST 承認済みのキーサイズを適用し、デバイスに使用されている SSL ソフトウェアで強力なキーを作成するための手順とコードのサンプルが推奨されました。

- **リスク 2:** デバイスに保存されているシステムユーザーパスワードが、比較的簡単に元に戻すことができる安全でないアルゴリズムを使用してハッシュされていたため、攻撃者によってデバイスにアクセスされる可能性がありました。
  解決ガイダンス: ユーザーパスワードに安全なハッシュアルゴリズムを使用すると同時に、既存のパスワードに期限を設けて更新を強制するよう OS を設定するための、具体的な手順が提示されました。

- **CVE:** デバイスで使用されていた Linux のカーネルのバージョンには、一般に広く知られている脆弱性がありました。これにより、特権を持たないローカルの攻撃者がルートレベルのアクセスを取得し、デバイスを制御できる可能性がありました。この脆弱性を解決するためのパッチが適用されていないことが判明しました。
  解決ガイダンス: カーネルのアップグレードによる完全な解決、パッチによる解決、デバイスへのリモートアクセスを無効にすることによる解決、不正なバイナリーの実行を防止するための Vdoo ERA（埋め込み型ランタイムエージェント）による解決を含む、4 つのオプションが提示されました。

分析結果を取得し、開発チームは Vision のガイダンスを使用してハイインパクトの問題を解決するための次の段階に移りました。その結果、6 日以内にほとんどの問題が解決されました。残る課題は、Linux カーネルに検出されたハイインパクトの脆弱性に関するものでした。これらを解決するためのカーネルのアップグレードは、非常に複雑でリスクが高いと考えられました。

初回の問題解決の後、2 回目の分析が行われました。この分析により、Linux カーネルを除くすべてのハイインパクトのリスクと CVE が、予想通り解決されたことが確認されました。

最後に、チームは残りの脆弱性の解決方法を検討し、Vdoo ERA の使用を検討することに決めました。

Vdoo ERA（常時稼働エージェント）によるシンプルな問題解決

このベンダーは、既存のデバイスコードを変更するリスクや手間を避け、Vdoo ERA による Linux カーネルの脆弱性の解決を検討することにしました。

同社は Vision で直接自動的にデバイス専用に最適化された ERA エージェントを作成し、簡単なプロセスでデバイスにエージェントをインストールしました。その後、自社のラボによるテストで、デバイスのパフォーマンスや機能が低下していないことが確認されました。

まとめ

Vdoo プラットフォームを使用することで、このお客様は次のようなメリットを得ることができました。

- **競争上の優位性** – 主力製品の迅速かつ大幅なセキュリティ強化により、セキュアなルーターとしての定評を得ることができました。
- **リスクの低減** – 詳細な可視性、ガイダンス、ツールにより、社内のセキュリティリソースを必要とせずに主な問題を解決できました。
- **効率化** – 最優先の問題を自動的に特定しガイダンスを得ることで、開発者による迅速な問題の解決が可能になりました。

このベンダーは、このプロジェクトで対象となった製品の改善だけでなく、今回の分析結果を使用してこのルーターと同じコードが使用されている類似製品のセキュリティも即座に改善し、その経験を活かして将来のセキュリティ対策を加速させることにも成功しました。

Vdoo について

Vdoo は自動デバイスセキュリティプラットフォームを提供し、企業による IoT、接続型、埋め込み型デバイスの、開発から導入後までを網羅した最善のセキュリティの迅速かつ大規模な実現をサポートしています。Vdoo は、サイバーセキュリティ企業の Cyvera 社を Palo Alto Networks 社に売却し、エンドポイントおよび埋め込み型システムのセキュリティに関する豊富な知識を持ちあわせた数人の起業家によって設立されました。Vdoo は、83North、Dell、WRVI、GGV、NTT ドコモ、MS&AD 各社をはじめとするトップレベルの投資　　家の支援を受けています。Vdoo は米国、ヨーロッパ、日本、イスラエルにオフィスを構え、世界的に有名な多数のお客様にご利用いただいています。

詳細につきましては、japan_info@vdoo.com にお問い合わせいただくか、弊社ウェブサイト https://www.vdoo.jp をご覧ください。