組み込みソフトウェア・テスト

リソースに制約のある環境での脆弱性テスト

組み込みデバイスのソフトウェアの不具合は、人々の生命や生活を支えるシステムの信頼性に多大な影響を及ぼす可能性があります。テストが組み込みシステムの開発プロセスにとって欠かせない要素なのはそのためです。システムを開発する場合は、常に妥協が必要なことは理解していますし、すべてのリソースのバランスを取って厳しい納期を守ることが簡単ではないことも承知しています。リソースのバランスを取るために必要なのは、事業にとって最も重要な不具合を効率的に特定するためにリスクに基づくアプローチを取ることです。

ブラック・ダックは一歩先を行きます

ATM から自動車、医療用装置に至るまで、設計で考慮された環境による組み込みデバイス固有のリソース制約やセキュリティ問題について通じており、また以下の制限を効果的にテストするのに必要とされる深い専門知識も有しています。

- ライフサイクルの長さ
- ユーザーの操作制限、またはユーザーの不介入
- 安全性の低い物理環境
- 規制上の課題
- 電源に関する制限
- 他のデバイスとの接続性
- 保守の制限

目標達成を支援します

各評価の最後に、お客様の開発チームとレビューを実施して以下の説明をします。

- 脆弱性ごとの説明
- 再現手順（該当する場合、エクスプロイトコードを含む）
- スクリーンショット（該当する場合）
- 攻撃者のスキルとアクセス権に基づいて問題が悪用される可能性
- 脆弱性の悪用に成功した場合の影響
- 可能性と影響度を組み合わせた標準ベースのリスク評価
- 組み込みデバイス固有の制約に対処するようカスタマイズされた 1 つまたは複数の推奨緩和策

3 つ分析手順を組み合わせるリスクベースのアプローチ

組み込みソフトウェアテストプロセスでは、以下の 3 つの領域に対応するリスクベースのシステムアプローチを取ります。

通信解析

他のローカルコンポーネントまたはリモートコンポーネントとの通信をエキスパートが傍受して解析します（該当する場合）。デバイスのソフトウェアによっては、最初にクライアントに対する特権アクセスを取得しないで可能な場合と、不可能な場合があります（例えば、信頼された CA 証明書をデバイスにインストールする必要がある場合もあります）。この手順には、USB、シリアル、イーサネット、POTS、Wi-Fi、セルラーなどのインターフェースによる通信が必要な場合もありますが、組み込みデバイスでよく使用される通信プロトコルに関しては多くの取り扱い経験があります。例えば、Bluetooth Low Energy、ZigBee だけでなくプロプライエタリなプロトコルも対応できます。

クライアント解析

優先度の高い領域をテストして、デバイス上の機密性の高いデータや機能へのアクセス権取得を試行し、特権昇格させて 1 つまたは複数の事業リスクに影響を及ぼす攻撃を実行できます。この段階の解析作業は、個別のデバイスや関連する攻撃への依存性が高く、チップ除去やリバースエンジニアリング／デバイスのファームウェアの改ざん、デバイスで動作するプロセスへのデータのファジング、カーネルレベルのエクスプロイトの検出などが含まれる場合もあります。

サーバー解析

クライアントとサーバー間の通信チャネルを傍受し、手動および自動のさまざまなツールを駆使してサーバーサイドソフトウェアを解析します。

ブラック・ダックについて

ブラック・ダックは、業界で最も包括的かつ強力で信頼できるアプリケーション・セキュリティ・ソリューション・ポートフォリオを提供します。ブラック・ダックには、世界中の組織がソフトウェアを迅速に保護し、開発環境にセキュリティを効率的に統合し、新しいテクノロジーで安全に革新できるよう支援してきた比類なき実績があります。ソフトウェア・セキュリティのリーダー、専門家、イノベーターとして認められているブラック・ダックは、ソフトウェアの信頼を築くために必要な要素をすべて備えています。詳しくは www.blackduck.com/jp をご覧ください。

ブラック・ダック・ソフトウェア合同会社

www.blackduck.com/jp