シック・クライアント・テスト

シック・クライアント・ソフトウェアの個別ニーズに応じてテストをカスタマイズ

シンプルな自動スキャンでは十分ではありません。

シック・クライアント・アプリケーションにはローカル処理とサーバー側の処理があり、プロプライエタリなプロトコルを使用して通信する場合が多いので、必要とされるセキュリティテストの手法も異なります。シンプルな自動スキャンによる脆弱性評価では十分ではありません。そのためアプリケーションに合わせてテストごとにカスタマイズするのです。

シック・クライアント・ソフトウェア同様にユニークな手法

シック・クライアント・アプリケーションのペネトレーション・テストでは、シック・クライアント・ソフトウェアおよび通信に使用するサーバーサイド API の両方をリスクベースで分析します。これにより以下の特定が可能になります。

- リスクの高いシステム領域
- 資産
- 攻撃者
- 考えられる攻撃経路

4つの分析方法を組み合わせたリスクベースのアプローチ

シック・クライアント・ソフトウェアのテストプロセスで取られるリスクベースの手法は、以下の 4 つの領域に対応しています。

1.コンフィグレーション解析

エキスパートがシック・クライアントのコンフィグレーションを解析し、デフォルトコンフィグレーションの問題だけでなく、セキュリティ制御を回避するようにアプリケーションが構成される恐れのある方法もあぶり出します。

2.ネットワーク通信解析

多くのシック・クライアントで懸念すべき攻撃のほとんどがリモートで実行可能なものです。その場合は、ネットワーク通信を傍受して詳細に解析します。

3.サーバー解析

ほとんどのシック・クライアントの本来の目的は、サーバー側の機能の一部を取り出すことです。サーバーサイドコードの脆弱性が重要である場合が多いのは、エクスプロイトに成功するとすべてのシック・クライアントや中央のデータストアに影響を及ぼす可能性があるからです。この段階では、手動および自動のさまざまなツールを使ってサーバーソフトウェアを解析します。

このアプローチには、ペネトレーション・テスト計画の作成による、リスクベースのテストシナリオの洗い出しと優先順位付けが含まれます。

4.クライアント解析

シック・クライアント・ソフトウェア自体の解析にはさまざまなツールを使用します。この段階の解析作業は、個別のソフトウェアと懸念すべき攻撃に大きく依存します。また、メモリダンプの実行、特権昇格を許可する可能性のある IPC チャネルのテスト、ファジングファイルの入力、徹底的なリバースエンジニアリングなどの作業を伴うこともあります。

最後までお客様をサポートします

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、以下について説明します。

- 評価ポイント
- 悪用の可能性と悪用された場合の影響に基づいた脆弱性の優先順位付け
- 脆弱性ごとの緩和策のアドバイス

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