CAN、CAN FD 対応
第 2 世代のファジングツール
beSTORM

beSTORM は、通信プロトコル定義に基づいて全ての対象フィールドに対するファジングテストを自動生成・実行するソフトウェアです。
beSTORM により、ソフトウェアの未知の脆弱性を開発段階で発見し、セキュア性能の高い製品開発が可能となります。

beSTORM(ビーストーム)の特長:

- 可能性のある全組合せをテストし未知の脆弱性を発見
- CAN、CAN FD 等、車載機器向けプロトコルに対応
- あらゆるネットワーク・アプリケーションをテスト
- 250 以上のプロトコルに対応済
- 独自プロトコル向けテストを迅速に実施可能
- 独自モニタ向けフレームワーク(API)を提供
- ISASecure「EDSA 認証 V.2.0.0 CRT ツール認定」取得
- ISASecure「SSA 認証 V.2.0.0 CRT ツール認定」取得

beSTORM 概要

1. 第 2 世代のファジングツール

「beSTORM」は、ソフトウェア製品の新しい未知の脆弱性を検出するために、プ ロトコルの構造に基いて可能性のある全ての攻撃を行います。この点が、アタックのシグネチャを用いたり、既知の脆弱性を発見しようとする旧世代のツールと全く異なるところです。

2. 車載機器向けプロトコルのサポート

CAN、CANFD の他、Wi-Fi, Bluetooth, USB,ファイルファジング等、車載機器で使用されるプロトコルのファジングテストに対応しています。

3. 高度な拡張性

XML によるカスタムプロトコル定義に加え、DLL 呼び出し機能により、テストを柔軟にカスタマイズできます。
カスタムモニタ用の API が提供されており、独自のモニターを作成し、「beSTORM」と連携させることが出来ます。

4. 柔軟なカスタムプロトコル対応

カスタムプロトコルのテストを容易に作成、編集、実行することができます。パケットキャプチャを使ったプロトコル定義から自動でテスト用の攻撃を生成することで、効率的なテストを短期間で実現します。

5. プロトコル定義内容の全てをチェック

RFC によるプロトコル定義から攻撃を生成し実行します。これにより、システムの機能全体がチェックされる事を確実にし、また、製品が市場に リリースされた後、数ヶ月、あるいは数年後に表面化することになるような脆弱性を素早く発見する事を可能にしています

6. マルチプロトコルサポート

全てのインターネットプロトコルが、「beSTORM」でテスト可能です。

7. 開発言語への非依存

「beSTORM」はバイナリ、アプリケーションをテストします。したがって使われているプログラミング言語やシステムライブラリを問題にしません。 「beSTORM」は、どのようにすると脆弱性が発現するかを正確にレポートし、プログラマーがアプリケーションのデバックを行うことを可能にします。
どのような開 発環境であるかは問いません。

8. 実際の攻撃によるテスト、正確なレポート

「beSTORM」は、実際の攻撃を実行することで、外部からアプリケーションをチェックし、例えばバッファオーバーフローが起こされたなど、実際に攻撃が成功した場合にのみ、脆弱性が報告されます。「beSTORM」は攻撃者をエミュレートするのです。攻撃者が攻撃に失敗した場合、beSTORM はそれをレポートしま せん。誤判定の数を効果的に低減させています。

9. わずかな例外でも検知

「beSTORM」モニタは、対象のプロセスにアタッチし、わずかな例外でも検知することで、脆弱性を検出します。これにより、「beSTORM」はオフ·バイ·ワンのような識別しにくい攻撃や、アプリケーションのクラッシュには至らないようなバッファオバーフローといった攻撃の発見が可能です

10. アタックの再現

「beSTORM」は、攻撃が成功した場合に、詳細なレポートを記録します。このレ ポートを使用することによって、その攻撃を再現することが可能です。また、Perl スクリプトで攻撃をエクスポートし、「beSTORM」の無い環境で簡単に攻撃を再現させることも可能です