脆弱性分析方法の具体例

【注意】
本資料は脆弱性分析手法の具体的な手法を単に紹介するものです
（ＣＣでは特定の分析手法の採用を推薦してはいません）

Flaw Hypothesis Method (FHM)

脆弱性分析書作成の問題点-方法論の不在

- ＣＣでは脆弱性分析の具体的な進め方に関する記述は殆どない（欠陥仮定法に若干触れている程度）。ＥＡＬ４以下では具体的な進め方を記載する必要もない
- ＥＡＬ５以上から具体的な進め方、方法論（系統的な脆弱性の探索方法、証拠資料の完全な分析（ＥＡＬ６以上））を脆弱性分析書に記載することを求めている

Flaw Hypothesis Method (FHM)

脆弱性分析書作成の問題点-方法論の不在

- しかしながらＥＡＬ5以上の評価は稀なため、具体的な方法論に関する認知度が低いのが現状
- 欠陥仮定法が最もＣＣの世界ではポピュラーな方法論。方法論自体は簡易でＥＡＬ4以下の評価に適用可能

Flaw Hypothesis Method (FHM)

欠陥仮定法とは

- 脆弱性分析を行うための手法論
- 以下の４フェーズにより構成
  - 想定される脆弱性のリスト（Flaw Generation)
  - 想定された脆弱性の検証（Flaw Confirmation)
  - 脆弱性の一般化（Flaw Generalization ）
  - 脆弱性の除去（Flaw Elimination)

Flaw Hypothesis Method (FHM)

欠陥仮定法とは

Flaw Generation	過去のTOE開発経験やTOEと同タイプの製品の公開された脆弱性情報をベースにTOEに想定される脆弱性をリストアップ
Flaw Confirmation	リストアップされた脆弱性がTOEに存在するか否かを確認。できうる限りテストはせず、机上での確認をメインとする
Flaw Generalization	TOEに存在すると確認された脆弱性（通常は詳細な情報を含む）を一般化し、他のコンポーネントに同種の脆弱性がないか確認する。
Flaw Elimination	脆弱性を実際に除去（コードの修正、設計書修正、マニュアル修正等）

Flaw Hypothesis Method (FHM)

公開情報を利用したFlaw Generation（Firewall)の例

Firewall Manager Discloses Firewall Passwords to Local Users

Description: Novacoast reports a vulnerability in the Cisco PIX Firewall Manager application that discloses the PIX device password to local users.
It is reported that PIX Firewall Manager will save the PIX firewall enable password in plaintext in an unencrypted log file when a successful connection is made. This log file apparently has no access restrictions.

- 同じ問題がTOEで生じることはないか？
- 他のTSFデータがログファイルに書き込まれることはないか？
- ログファイル以外は（デバックログ等）？

Flaw Hypothesis Method (FHM)

Flaw Generation/Confirmation

脆弱性ID：TOE14

リスク：大

リファレンス：外部仕様書　4.3章、14.1章

想定される脆弱性：ログファイル及びデバックログファイルにTSFデータが記載されてしまう

攻撃方法：ログ取得ON、デバックONに設定し、ログファイル・デバックログファイルを参照

Flaw Confirmation

分析結果：脆弱性の存在が確認された。
デバックログファイルにフィルタリングルール（管理者のみ閲覧可能）がログされる。デバックログファイルのディレクトリがアクセス制御されていない場合、権限のないものがフィルタリングルールを参照可能だが、ガイダンス文書にはその旨の記載がない

Flaw Hypothesis Method (FHM)

Flaw Generalization/Elimination

分析結果：脆弱性の存在が確認された。
デバックログファイルにフィルタリングルール（管理者のみ閲覧可能）がログされる。デバックログファイルのディレクトリがアクセス制御されていない場合、権限のないものがフィルタリングルールを参照可能だが、ガイダンス文書にはその旨の記載がない

Flaw Generalization

ログ生成関数の仕様に問題→他にこの関数を使用しているような機能は？
同じような仕様の関数は？

Flaw Elimination

仕様変更、もしくはマニュアルの修正等により、脆弱性の悪用を阻止

Flaw Hypothesis Method (FHM)

欠陥仮定法のメリット

- ＣＣでの実績
- ＥＡＬ４で実施される評価者による独立脆弱性分析への活用