脆弱性情報調整時の課題解決に向けて

JPCERT コーディネーションセンター

最近の脆弱性調整時で見られた課題

- 脆弱性調整において見受けられた課題
  - **課題１：インシデントの分析過程で新たな脆弱性が確認され、制度への届出に至ったケースでの情報流通への課題**
  - **課題２：脆弱性情報の公表日（45日目安） への課題**
  - **課題３：製品開発者による全顧客把握と通知問題に対する課題**
- こうした課題を解決していく上での解決策について議論・検討を行いたい

  今回は概要説明・問題提起のみとして、次回以降に議論・検討を進める予定
  （第1回：概要説明・問題提起、第２・３回：議論）

課題の背景（１ー概要）

- **インシデントの分析過程で新たな脆弱性が確認され、制度への届出に至ったケースでの情報流通への課題**
  - 届出時の段階でサイバー攻撃での悪用が判明していたもの 6件 (2019年-2021年)※JVN-JPおよびJVN-VUの取り扱いを合算
  - そのうち5件についてJVNアドバイザリ公表時に攻撃の発生（いわゆる「in the wild」表示）について触れた

- **脆弱性調整上の課題**
  - **制度（告示・ガイドライン）において脆弱性情報、脆弱性関連情報では明確な記載がない**
    - 一方でアドバイザリや注意喚起において利用者に速やかな対応を求めていく上で重要な情報
  - 調整において取り扱いが難しい（案件に応じた調整を実施）のが現状
    - 脆弱性がすでに悪用されていることが判明しているケースへの考慮
    - 発生しているコンピュータセキュリティインシデントへの対応や、各届出との切り分け
  - JVN アドバイザリにおいて、攻撃の発生について触れるケース、触れていないケースと、案件ごとに差が生じやすい

課題の背景（１ー現状の調整活動）

- **製品開発者の理解を求めて調整を実施**
  - **脆弱性悪用を認識している場合には、JVNへの掲載や注意喚起の発出について打診**
  - コンピュータセキュリティインシデントへの対応やその他届出についてJVNへの相談とは切り分けて対応することを誘導
  - **製品開発者とのJVNアドバイザリ、注意喚起の同意を得て進める**
    - 製品開発者によってはカスタマー対応の実施等、スケジュールを調整

- **課題**
  - **制度上では脆弱性悪用情報の取り扱いについて（具体的に）記されていない**
  - **製品開発者との調整において制度上で根拠となる記載が無いため、調整に苦慮するケースがある**

課題の背景（２ー概要）

- **脆弱性情報の公表日（45日目安） への課題**
  - **45日以内に公表した割合は、おおよそ30%程度でここ数年横ばいが続いている（大半が軽微な修正など）**
  - 45日の目安は、CERT/CC (自ら発見し、自ら調整を行う) 45-days disclosure policy を参考として設定されたもの
    - 今日では、Google (ソフトウェア、90日) , ZDI (ソフトウェア、制御、120日）など複数の目標値がある

- **公表日目安 (Timing of advisory release) 設定について**
  - ISO/IEC 29147 や、CERT/CC (The CERT® Guide to Coordinated Vulnerability Disclosure)での考え方
    - 利用者のために、解決策が利用可能になれば速やかな情報公開を進めることが望ましい
    - 脆弱性がすでに悪用されているケースではより迅速な対応が求められることが触れられている

課題の背景（２ー現状の調整活動）

- **公表日を（早める｜遅らせる）事由についての検討と、届出時での考慮されるポイントが乏しい**
  - 制度では、公表日決定について次の要素が考慮される
    - ①対策方法の作成に要する期間
    - ②海外の調整機関との調整に要する期間
    - ③脆弱性情報流出に係るリスク
  - 過去の類似事例などを踏まえつつ製品開発者と調整を進める
    - サイバー攻撃での悪用や、製品開発者の個別顧客対応など勘案

- **課題**
  - 攻撃での悪用など公表日決定に本質的な影響を与える項目が制度では記されていない
  - 制御・組み込み製品の現場では品質保証などの対応を含め対応に時間を要するケースもある
  - 製品開発者が問題解決に向けて努力していることが評価されにくい

課題の背景（３ー概要）

- **製品開発者による全顧客把握と通知問題に対する課題**
  - JVN 公表時での質問をいただくことがある (製品開発者にとっては一つの解決方法として認識されている)
  - 全顧客把握通知としてもトラブルがまったくないわけではない
  - 全顧客把握通知としなくとも、アドバイザリ公表とは別に製品開発者での連絡を並行して行い対策を進めているケースも多い

- **現在の調整活動**
  - 製品開発者との間でのヒアリング
  - 念書の確認と全顧客把握通知による取り扱い終了

本課題について検討の進め方について

- **製品開発者の問題意識の確認も必要**
  - 製品開発者にアンケートやヒアリング等進めることも検討

- **制度の変更が必要なポイントを含めて、課題解決に向けての脆弱性研究会での議論**
  - 課題と論点の再確認
    - **課題１：インシデントの分析過程で新たな脆弱性が確認され、制度への届出に至ったケースでの情報流通への課題**
      - 脆弱性届出に攻撃悪用に関する情報が含まれる場合、その情報の取り扱いや保護をどう進めるのが適切か？
    - **課題２：脆弱性情報の公表日（45日目安） への課題**
      - 公表日を定める条件の確認、現実に尺度となる目標の提示と、がんばっている製品開発者のエンカレッジ
    - **課題３：製品開発者による全顧客把握と通知問題に対する課題**
      - 製品開発者と利用者にとってよりよい形とするにはどのような工夫がありうるか？