脆弱性届出者のこぼれ話

株式会社ビジネス・アーキテクツ
太田 良典

Business Architects Inc.

受賞内容

- 第2回IPA賞 情報セキュリティ部門
- 受賞理由：
  - 「情報セキュリティ早期警戒パートナーシップ」において、脆弱性届出件数がいちばん多かった
- 届出件数 = 約120件

脆弱性

- コンピュータプログラムの不具合や設計ミスにより、安全が損なわれている状態
- たとえば：
  - 他人が入力した個人情報が読めてしまう
  - 会員用の機能が他人に使われてしまう
  - サイトが改竄されて攻撃の踏み台にされてしまう

発見するときのお話

どうして、どうやって発見するのか

Business Architects Inc.

どうして発見するの?

いつ何を発見したか考えてみると……

- タイミング
  - 仕事中に Web を見て発見していることが多い
- 内容
  - ほとんどが Web の脆弱性

仕事柄かも?

弊社のお仕事

Business Architects Inc.

- Webサイト構築が主業務
- 特に、大規模な企業サイトが得意
  - 事例 : http://www.b-architects.com/works/projects
- Webサイトを見るのも仕事のうち
  - 一見わからないが、品質の低いサイト → 嫌な予感

嫌な予感の一例

- スクリプトを有効にしたときのみ正常に動作
- スクリプト無効環境を考慮していない
  - 配慮がないばかりか、考慮もしていない
  - スクリプト無効環境でのテストを実施していない可能性が高い

軽く調査すると……

「予感」をどこまで確認するのか

- 確認するとサイト側に被害が出るケース
  - SQLインジェクションによるDB破壊
  - ディレクトリトラバーサルによる個人情報の漏洩
- 確認すると発見者側に被害が出るケース
  - ディレクトリトラバーサルでプログラムのソースが見えた
    → 不正アクセス禁止法違反容疑で家宅捜索

「寸止め」が重要

(確信が得られないこともあるが、仕方ない)

届出するときのお話

ノールールの時代から
「届出」の時代へ

Business Architects Inc.

昔の話：発見時の選択肢

- 見なかったことにする
  - 対応されない
  - やがて別の誰かが発見して悪用する危険性
- 公開する
  - 対応されるが、その前に悪用される危険性
- 管理者に直接通知する
  - 対応される……？

直接通知の問題点

- 連絡先がみつからない
- 連絡しても返事がない
- 話が通じない、認めない
  - 特に「寸止め」必須なため証拠が出せないケース
- 「逆ギレ」や無理難題
  - 「攻撃しないでください」
  - 「アクセス元のリモートホスト情報を全て提供してください」

とにかく面倒、精神的負担も大きい

「届出」という選択肢

- 2004年7月、届出制度の運用開始
- 意外に柔軟な対応
  - 「連絡先不明」でも受理される
  - 「脆弱性の疑い」だけでも受理される
    - 特に SQL インジェクションやディレクトリトラバーサルなど、寸止め必須なケース
  - 「脆弱性ではない」ケースに対応してくれる事も
    - 「脆弱性ではないが問題がある」場合、通知してくれる
- 精神的な負担が少ない

直接通知よりずっと楽

届出の問題点

- そもそもメールを書いて送るのが面倒
  - 楽なのは「直接連絡するのに比べれば」の話
  - 発見に至った経緯、脆弱性であると判断した理由など7項目を記入する必要あり
    (※ソフトウェアの場合はさらに項目が多い)
- PGPで暗号化するのが面倒
  - PGP / GPG に対応したメーラーが必要
  - Webフォームもありますが……

届出受付フォーム

届出の問題点(つづき)

- 届出すべきかどうか迷うケースがある
  - 「寸止め」で確信が持てないケース
  - 迷ったら届出で OK、と言ってもなかなか
- 届出できないケースもある
  - 仕事に関係あるもの
    - NDA(秘密保持契約)があるため、情報提供できず
  - 公開前のテスト中に発見
    - テスト結果として不具合報告
- 届出する気にならないケースも……？

届出する気にならないケース

spamメール
↓
URLに個人識別番号
↓
識別番号をでたらめなもの
に変えてアクセス
↓
脆弱性疑惑

- 脆弱性が修正されると
Webサイトが安全になる?

届出した後のお話

さまざまな結末と
個人的な願い

Business Architects Inc.

とあるケース

- あるサイトの脆弱性3件を届出
- 届出から数日後、たいへん丁寧な謝辞
- 約1ヵ月から1ヶ月半で随時修正
- 修正完了後、サイト上に詳細なアナウンス
  - おわび、脆弱性の内容、今後の対策

届出者冥利につきる

厳しい現実

- 修正されても公表されないことがほとんど
  - いわば「闇改修」
- 個人情報漏洩の可能性があったケースも公表されない
  - ガイドラインでは公表することになっている
  - が、現実には……
    - 調査もしないで「実害なし」「公表の必要なし」と判断している?
    - 本当に調査したのであれば、「漏れていない」ということを公表してほしい (一利用者として)

情報が公開されないと……

- 対応策が実施できない
  - 例：パスワードが盗まれていた可能性
    →パスワードを変更すれば OK
- 脆弱性の対策が進まない
- 発見者にとっても精神的な負担
  - 自分だけが知っているプレッシャー (ロバの耳)
  - 自分だけ対応策をとっている罪悪感

発見者はいらいら、やきもき

グッドニュース?

- 調整機関自らが情報公開の手本を示した例
- 脆弱性の専門家でさえ、脆弱性を指摘される
  - 脆弱性はどこにでもある
  - 恥ではない
- 情報公開しやすい空気……を期待

ありがとうございました

資料等は……

脆弱性届出者のこぼれ話@IPAX2006

http://bakera.jp/ipax2006/