2008年の脆弱性傾向と今後の課題

コーディネーションセンターの立場から

2008-11-27

JPCERT/CC
宮地 利雄

本日のアジェンダ

JPCERT CC®

- JVN この1年間の動き
- この1年間にJVNで公表された脆弱性

[傾向と課題]

1. 多いクロス・サイト・スクリプティングの脆弱性
2. オープン・ソース・ソフトウェアの多様性と脆弱性
3. セキュリティ仕様が明確になっていないインターフェース
4. 制御系システムの脆弱性

Copyright© 2008 JPCERT/CC All rights reserved.

JVN この1年間の動き

- 「情報セキュリティ早期警戒パートナーシップ」が4年を経過
  - 重要インフラ事業者への優先情報提供を模索
- 国際化に向けた元年
  - JVN英語サイト開設
    http://jvn.jp/en/
    (2008年5月)
  - CVE番号の原則取得を開始
    CVE：Common Vulnerability Enumeration
    (2008年9月より)
  - 脆弱性開示に関する国際標準検討開始
    ISO/IEC 29147
    (2008年4月より)

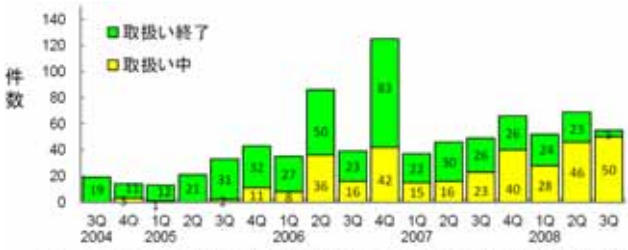


図2. ソフトウェア製品に関して各四半期に届出のあったものの現在の状況

Copyright© 2008 JPCERT/CC All rights reserved.

この1年間にJVNで公表された脆弱性

対象期間：2007年11月～2008年10月

- 総数：137件
- 報告元
  - 国内が多数：92件 (67%)
  - CERT/CC(米国)：44件 (32%)
  - CPNI(英国)：1件 (1%)
- 脆弱性の内訳(種類)
  - XSSがもっとも多い：51件 (37%)
  - バッファー・オーバーフロー：23件 (17%)
- 製品の内訳(種類)
  - グループウェア：12件 (9%)
  - ECシステム：8件 (6%)
  - マルチメディア・プレーヤー：8件 (6%)
  - ブラウザー：7件 (5%)
  - ウェブ・サーバ：6件 (4%)
  - セキュリティ製品：6件 (4%)
  - 制御系システム：5件 (4%)
  - コンテンツ管理システム：3件 (2%)
  - IPv6：3件 (2%)
  - PDF関連：3件 (2%)
  - 圧縮・解凍ツール：3件 (2%)
  - 印刷：3件 (2%)
  - 掲示板システム：3件 (2%)
  - ルーター：3件 (2%)

Copyright© 2008 JPCERT/CC All rights reserved.

1) クロス・サイト・スクリプティングの脆弱性

JPCERT CC®

- ウェブ・サイトだけではない「クロス・サイト・スクリプティングの脆弱性」
  - 「製品の脆弱性」においても多数を占める
    - JVNで公表された脆弱性の37%
      (CERT/CCでは取扱い対象にしていない)
    - 国内で報告された脆弱性の55%

- 典型的な影響ある製品
  グループウェア, ECサイト構築ソフト,
  各種製品の管理用インターフェースなど

- 製品開発者も安全なウェブの作り方の学習を！
  - 安全なウェブサイトの作り方　改訂第3版
    (http://www.ipa.go.jp/security/vuln/documents/website_security.pdf)

Copyright© 2008 JPCERT/CC All rights reserved.

2) オープン・ソース・ソフトウェアの脆弱性

JPCERT CC®

- オープン・ソース・ソフトウェアの多様性
  - サンプル・コード(保守なし)のつもりで公開されているソフトウェアも多い
  - 開発者に連絡が取れないケースも少なくない
  - 脆弱なソフトウェアがダウンロードされて使われ続けるケースも

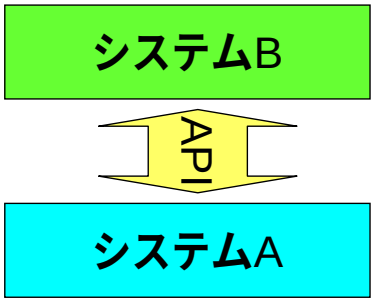
- 利用時の注意
  - 保守されているソフトウェアなのかどうかを見極めて利用しよう！

- JVNでの取扱い
  - 開発者と連絡が取れない場合には:
    (現状は) 取扱いを終了する
    (検討中) 総合的に判断した上で原則として公表する

Copyright© 2008 JPCERT/CC All rights reserved.

3) 明確になっていないセキュリティ仕様

- システム間インターフェースにおける不明確なセキュリティ仕様
  例) ブラウザ ～ プラグイン･ソフトウェア
  - 仕様が文書化されていない
    あるいは
    仕様の中で言及されていない
    - 定義域チェックは誰の責任？
    - 特殊記号の無視：小さな親切が大きな迷惑



- 全体最適とならない決着も
  - 現実には，どちらのシステム側で手当てをするかは，両システムの開発者の力関係で決まってしまう

Copyright® 2008 JPCERT/CC All rights reserved.

4) 制御系システムの脆弱性

- JVNでも5件の脆弱性を公表

- オープン化が始まった制御系システム
  - オープン化の進展に伴うセキュリティ問題の顕在化
  - 情報系システムとも接点ができる

- 制御系システムの固有の課題
  - 高い応答性と信頼性，運用継続性が期待されている
  - 組込みシステムの比率が高い
    → 改版に手間取るファームウェア等
  - 人命にかかわる事故につながる可能性

- 制御系システムの脆弱性の公表はいかにあるべきか？

• 情報系システム領域での知見を活用して問題解決を！

• 情報系システム担当者も無縁ではない！

Copyright® 2008 JPCERT/CC All rights reserved.

今後とも御協力をお願いします！

JPCERT CC®

情報セキュリティ早期警戒パートナーシップは，関係の皆様の
御協力に支えられて成り立っています．

脆弱性研究者

脆弱性発見者

製品開発者

利用者

システム管理者

今後ともご支援とご協力をお願い致します！

Copyright® 2008 JPCERT/CC All rights reserved.