RSA Conference Japan 2008で利用したスライドです

フリーソフトウェアと脆弱性情報流通

鈴木裕信 | 特定非営利活動法人フリーソフトウェアイニシアティブ | 2008年4月24日 | C4-2

Agenda

- WHO AM I?
- What is Free Software?
- Myth of Free Software
- What is Distribution?
- Distributions
- Foo Bar Community
- Free Software Projects
- Competitor and Survivors
- Software Vulnerability (and Software Engineering)
- Process of Vulnerability Handing in General
- CSIRTs and Communities
- Security Update
- Topics
- Conclusion
- Q&A

WHOAMI

- 鈴木裕信（すずきひろのぶ）
  - 鈴木裕信事務所有限会社取締役社長
    - 大学講師等
  - 特定非営利活動法人フリーソフトウェアイニシアティブ　副理事長・事務局長
    - 今日はこの帽子で
  - 中間法人JPCERTコーディネーションセンター理事
  - ソフトウェア技術者協会幹事

略歴

- 85年:UNIXを使いたくて株式会社SRAに入社
  - 開発現場でバブル絶頂期を経験
- 90年:ソフトウェア工学研究所へ異動
  - ネットワークトラフィックの研究・ソフトウェア品質の研究
- 96年:ソフトウェアコンサルタントとして独立
- 近年の主な研究活動
  - 信頼できるOpenPGP公開鍵サーバOpenPKSD Trusted Key Serverの研究開発 http://www.openpksd.org
  - 早期広域攻撃警戒システムWCLSCANの研究開発 http://www.wclscan.org

What is FSIJ

- 特定非営利活動法人フリーソフトウェアイニシアティブ
  - The Free Software Initiative of Japan

FSIJは、個の創造性発揮によって、経済・文化の発展に寄与することを目的に、開発者・利用者を支援し、正しいフリーソフトウェア概念の普及に努めるとともに、国際シンポジウム開催などの活動を行ない、高品質なフリーソフトウェアを日本から発信していきます。

http://www.fsij.org/

What is Free Software？

- ４つの自由を持つソフトウェア
  - 第0の自由：目的を問わず、プログラムを実行する自由
  - 第1の自由：プログラムがどのように動作しているか研究し、そのプログラムに必要に応じて修正を加え、採り入れる自由
  - 第2の自由：プログラムのコピーを再頒布する自由
  - 第3の自由：プログラムを改良し、自らの改良点を公衆に発表する自由

Typical type of Free Software

- GNU General Public License (v2 or v3)で運用されるソフトウェア
  - Linux, GCC, MySQL, etc.
- GPL v2/v3互換のライセンスで運用されるソフトウェア
  - Apache License, Version 2.0
  - FreeBSD license
  - Intel Open Source License
  - Blah,blah,blah…

Free Software vs. Open Source

- Open Source は市場開拓のためFree Softwareをcompromiseした用語
- オレ様Open Sourceが多すぎ混乱している
  - OSI認定ライセンスの氾濫
- Linuxはオープンソース？
  - GPL適用のフリーソフトウェアというのが真実

Myth of Free Software

ルールが違うGAME

- ライセンスかよくわからないソフトウェア
  - GNU General Public License v2/v3あるいは互換のライセンスを持つソフトウェア
- 誰が作っているのかわからないソフトウェア
  - コミュニティが作り出すソフトウェア
- 無料のソフトウェア
  - データベースMySQLは商用でかつGPLライセンス

What is Distribution?

- カーネル・ミドルウェア・アプリケーションがセットになっている環境
  - ドキュメントツールからウェブサーバまで、インストールからソフトウェアアップデートまでトータルパッケージとして提供される
- 何を選ぶか、どうセッティングされているかはディストリビューション毎に違う
  - ユーザターゲットと流儀の違い

Distributions

- Debian GNU/Linux
  - Ubuntu
    - Kubuntu
    - Edubuntu
    - Xubuntu
  - KNOPPIX
  - Xandros
  - gOS
- Gentoo Linux
- Fedora (Radhat)
  - Red Hat Enterprise Linux
  - CentOS
  - Yellow Dog Linux
- Mandriva Linux
- openSUSE
- MEPIS Linux
- Slackware Linux
- Vine Linux

Foo Bar Community

- コミュニティにより作り上げる
  - 企業活動 (Canonical, Redhat, Novel, IBM, HP, Google, etc…)
  - 成果のフィードバック (研究所, 大学, 企業)
  - ボランティア(学生・エンジニア)
    - スキルアップとキャリアを重ねることができる
- コミュニティのメタな組織化
  - The Free Software Foundation
  - SOFTWARE IN THE PUBLIC INTEREST, INC

Free Software Projects

- Debian Project
  - 主要Linuxディストリビューションの中でも最大級のパッケージ数を誇り、組織も巨大
    - パッケージ数：～18000
- GCC Project
  - もっとも進化した開発コミュニティの形

Debian Project : well-defined structure

- 明確な組織体系
  - 細部にまでかなりきめ細かく責任範囲が明確
  - ほとんど企業体とかわらない組織体系
    - http://www.jp.debian.org/intro/organization
  - Debian maintainerとなる参加プロセスが明確
- 明確な管理プロセス
  - 品質保証やセキュリティ部門をもち明確な管理プロセスの制定
  - セキュリティ監査とセキュリティーチーム
    - Debian Security Announcement の発行
    - Open Vulnerability and Assessment Language の主要メンバー
      - http://oval.mitre.org/

GCC Project : flexible structure

- Steering Committee : 15
- Maintainers
  - Blanket Write Privs: 11
  - CPU Port: 60
  - OS Port: 16
  - Language FE: 15
  - Various: 81
  - Non-Algorithmic: 6
  - Reviewers: 17
  - Write After Approval: 182
- Role-Based Classification
  - Release Managers: 1 + 3
  - Language Lawyers
  - Bugmasters
  - Sweepers
  - Housekeepers

Competitors and Survivors

Alternativeが存在する強さ

- 競争原理と生き残り
  - 問題があれば、次のものが簡単に取ってかわる
  - お互いが競い合い完成度の高いもののみ生き残れる
- ユーザは厳しい
  - まともにメンテナンスできていないようなソフトウェアなら、別のものを使えるからいらない

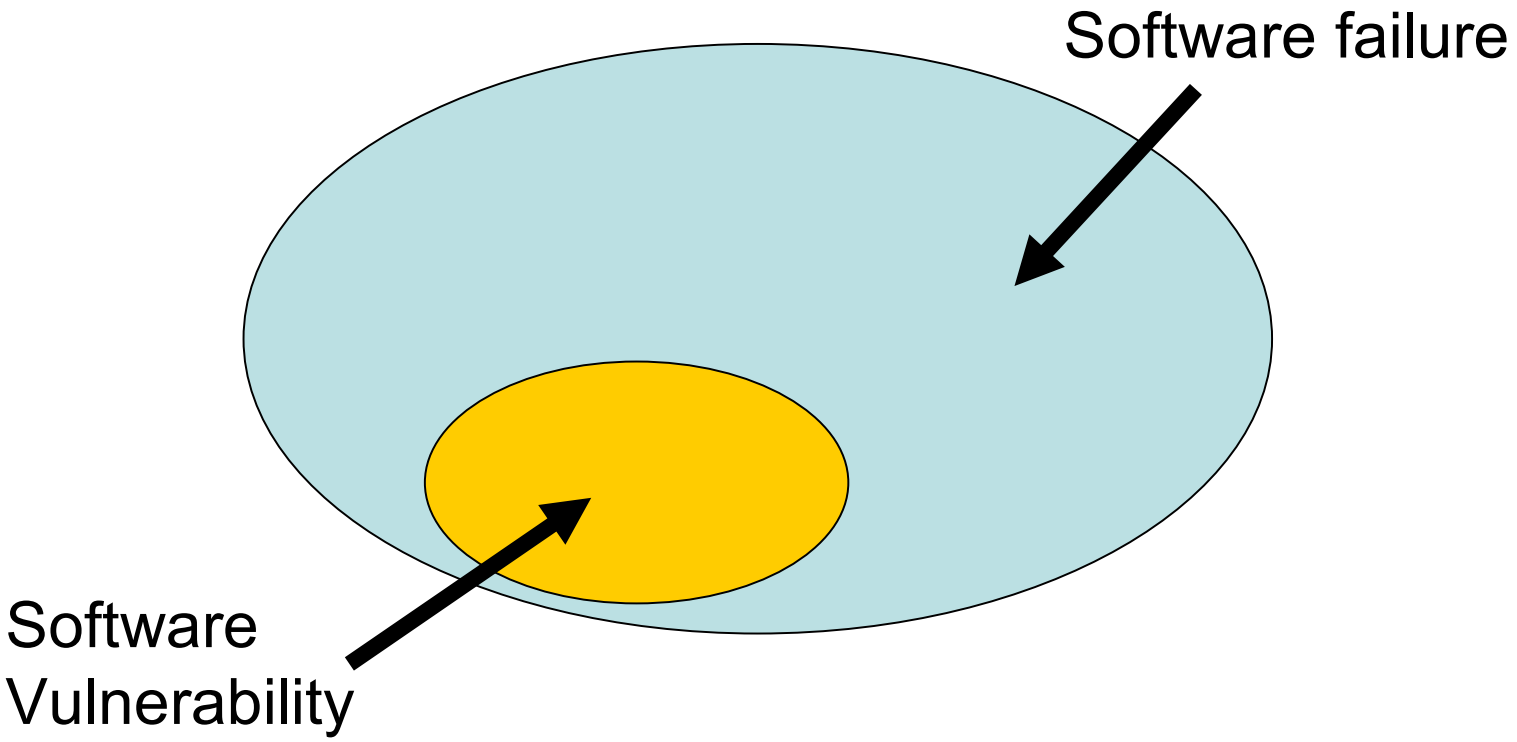
Competition

- メールシステム
  - sendmail
    - 初期のインターネットの時代からのMail Transfer Agent
  - postfix
    - Wietse Venema's MTA
      - IBM Secure Mailer とも呼ばれIBMがオープンソースに乗り出すきっかけを作った
  - qmail
    - Dan J. Bernstein's MTA
  - exim
    - Developed at the University of Cambridge

熾烈な開発競争

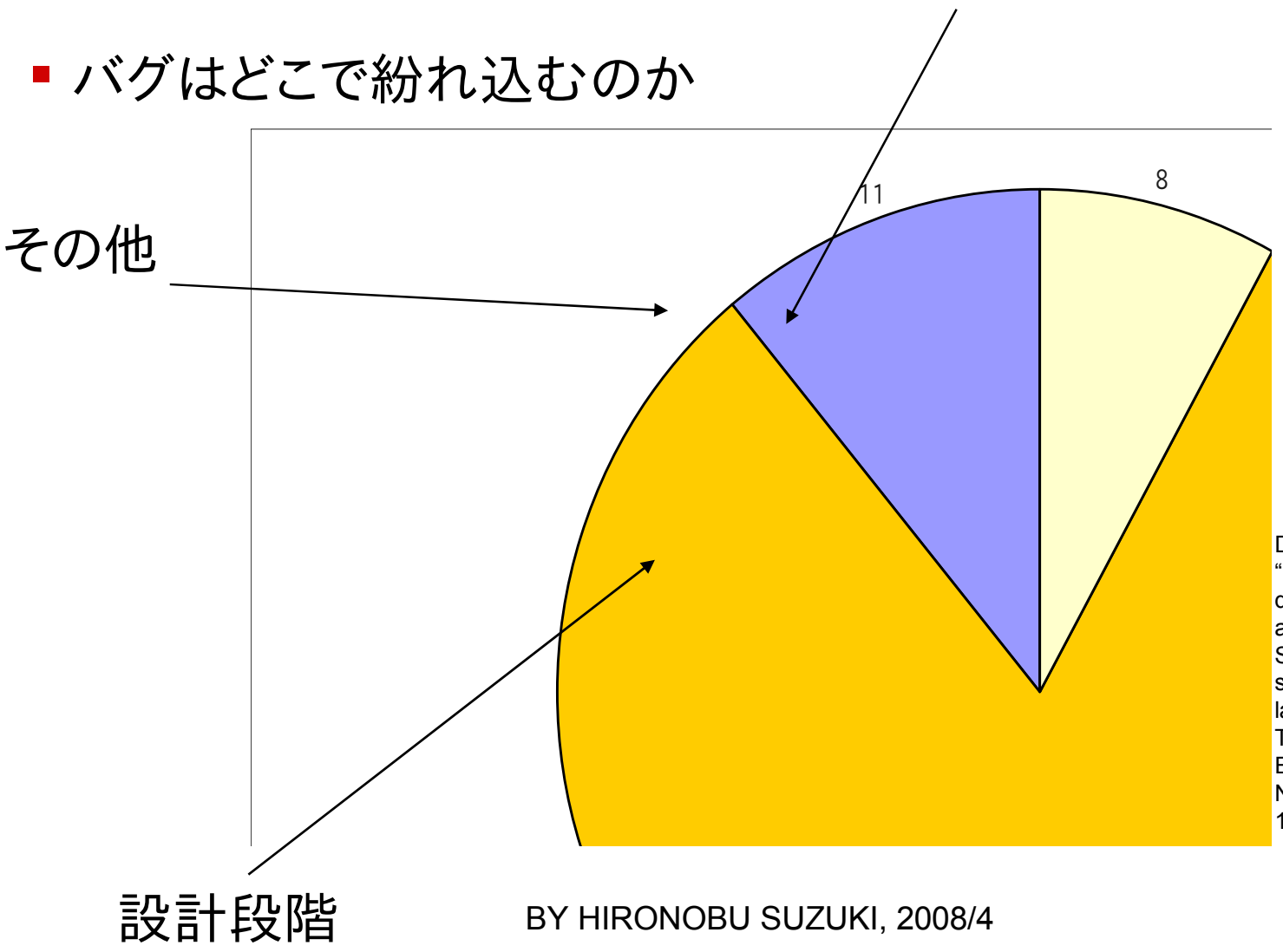
Software Vulnerability

- 第三者によるセキュリティ侵害を行うことが可能なソフトウェア故障(Software failure）



Software Engineering

- バグはどこで紛れ込むのか



D.M. Weiss et al., “Evaluation software development by analysis of changes: Some data from software engineering laboratory”. IEEE Trans. Software Engineering, Vol. 11, No.2 pp.157-168, Mar., 1985

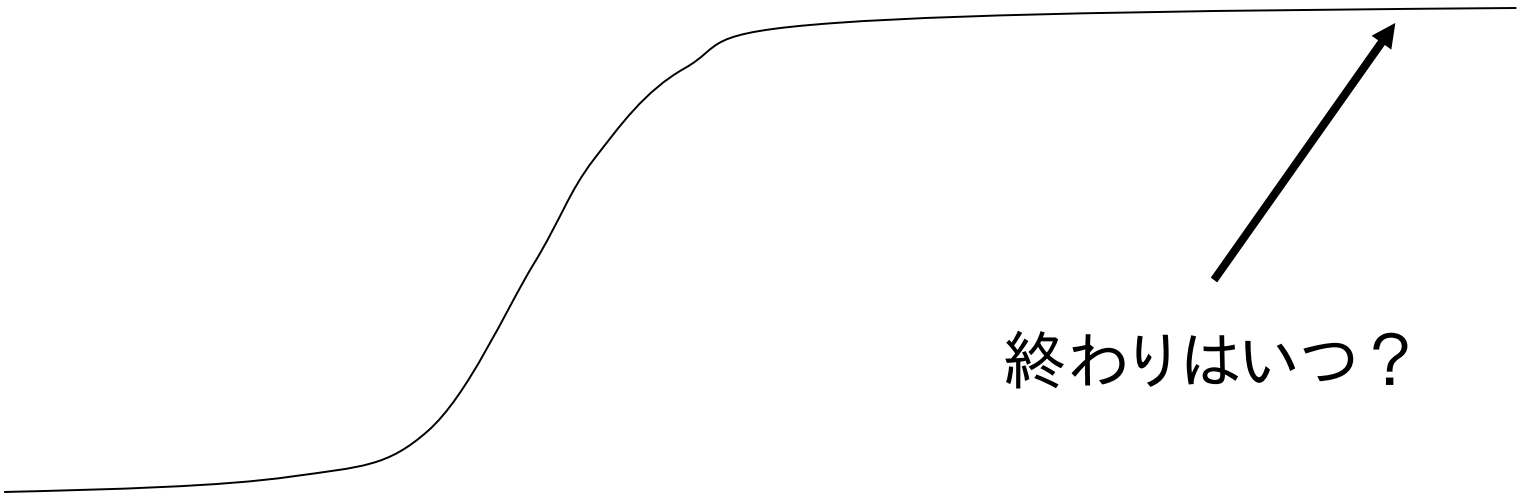
Software Engineering

IBM Research Journal, 28, pp2—14, 1984

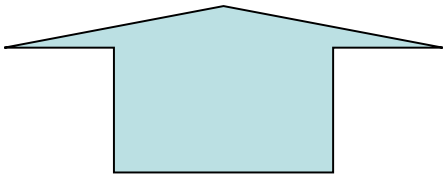
- バグの30% は5000年実行時間に対し1度現れる頻度

S字型ソフトウェア信頼性成長モデル

- バグの死滅はロジスティック曲線



- ブラックボックス･テスト
  - ソフトウェアの中身がどのように実装されているかはタッチせずブラックボックスとし仕様にしたがってテストしていく



ソースコードの存在は関係ない

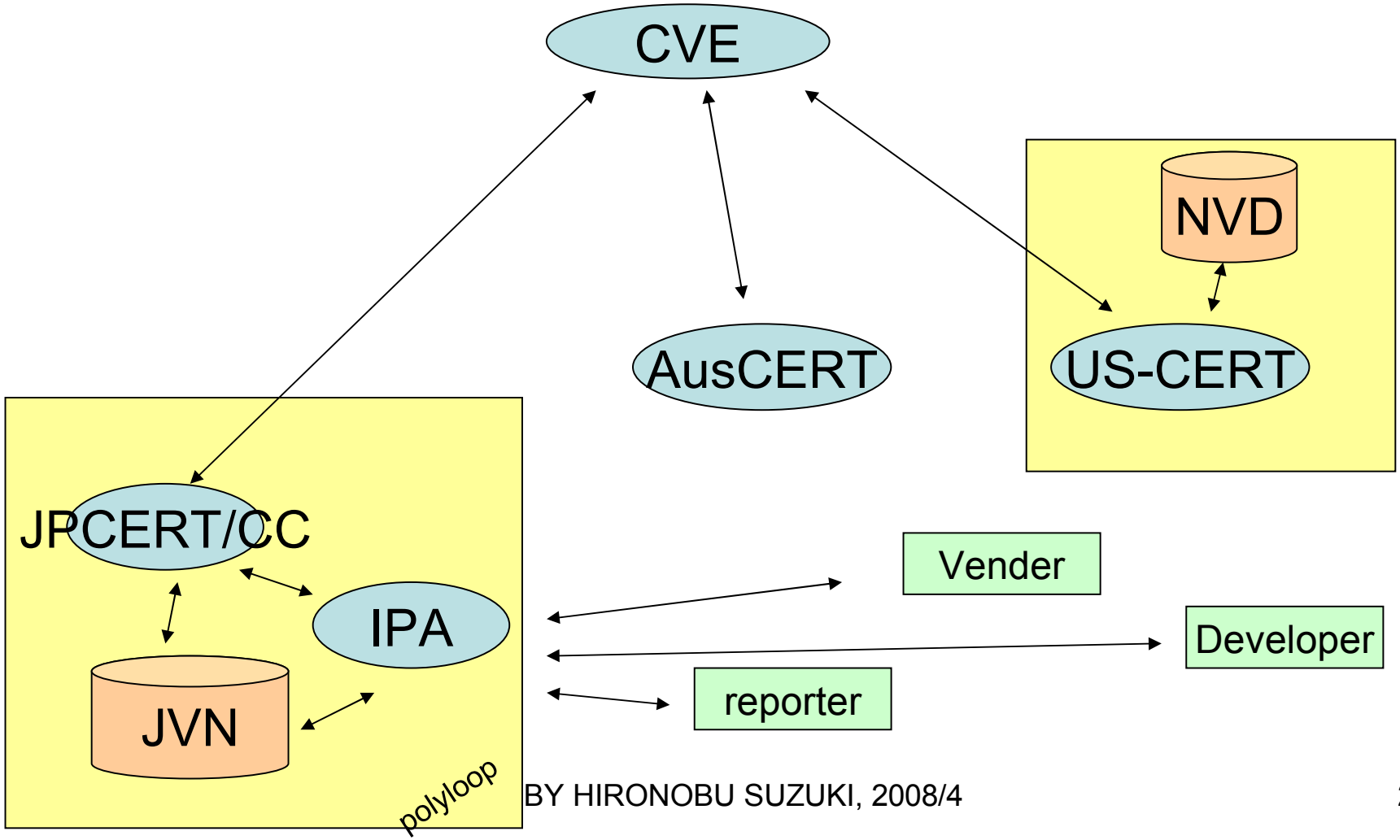
ソフトウェア工学的視点から

あたりまえのことを明確にいうと

- 中身を隠していようとも、どんなに使われていようと、時間がたっていようとも、ある日、あるとき、設計段階に起因する脆弱性が突然現れることを想定しなければならない
- 脆弱性を見つけることもできると考えるべき
  - ブラックボックステスト手法でSoftware Failureを探し当てた、その中の一部は脆弱性である
  - 成長モデルの観点からいえば、ソフトウェアのサイズに依存する

Process of Vulnerability Handing in General

Mitre common vulnerabilities and Exposure

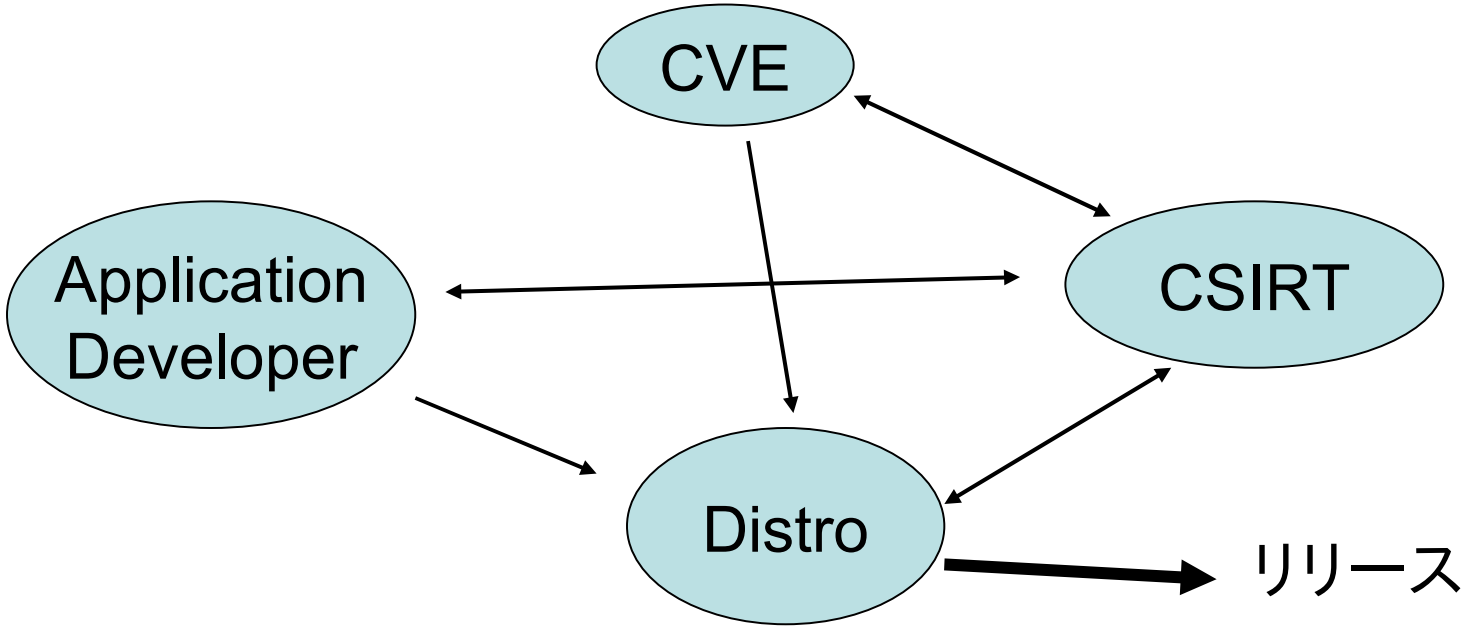


CVE　(Mitre Common Vulnerability Exposure)

- 米国土安全保障省 (Department of Homeland Security)がスポンサー
- 最終的に、ここに登録されて、正式な脆弱性と認知される
  - 逆にいえばCVEのIDをもらえないと正式な脆弱性扱いしてくれない
    - 経験から言えばディストリビューションの脆弱性をローカルで修正してもCVEが取られていなければ、それは本体に反映されない

CSIRTs and Communities

- CVEに登録されたら関係するCSIRT間で連絡を取りコミュニティに情報がフィードバックされる



Small Group Developers

アンテナとどかない

- コミュニティも作れないような小規模なソフトウェア開発グループ・開発者はこのルーティーンの中に入れない
- 当然Vul Handling もよくわからない
  - 本格的にやろうとするとかなり負担になるのは事実
- 国内のフリーソフトウェアコミュニティの基点となりうるFSIJに期待される役割
  - 日本国内のフリーソフトウェア開発グループにはFSIJがリーチできるよう努力する

Dilemma

- 大手開発コミュニティは内部ですべて処理できる
- 小規模な開発グループはむずかしい
  - そんなにポピュラーではない
  - さらにうまくハンドルできない
  - 人気が下る
  - 負のスパイラル

競争の過程で滅ぶべきものなのか、救うべきものなのか～ジレンマが存在する

Security Update

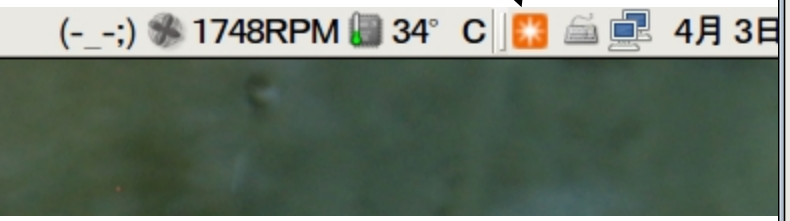
- ユーザに自動的に通知
  - ユーザは自分の判断でアップデートするかどうか決める
    - 強制的にupdateさせるわけではない
  - ダブルクリックで済みます

わからないことだらけ？
でも安心できるの

1ユーザとしての本音

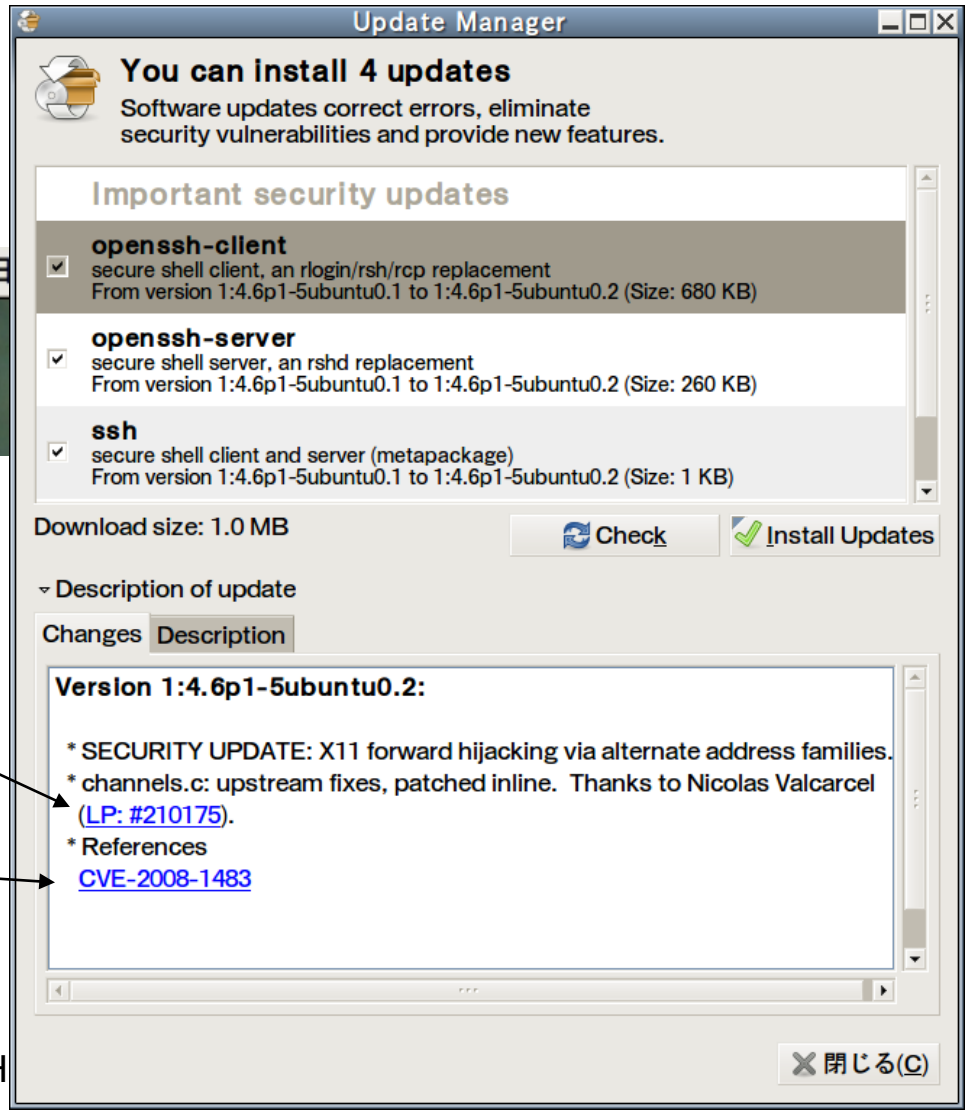
Security Update (Ubuntu)

Updateを知らせる

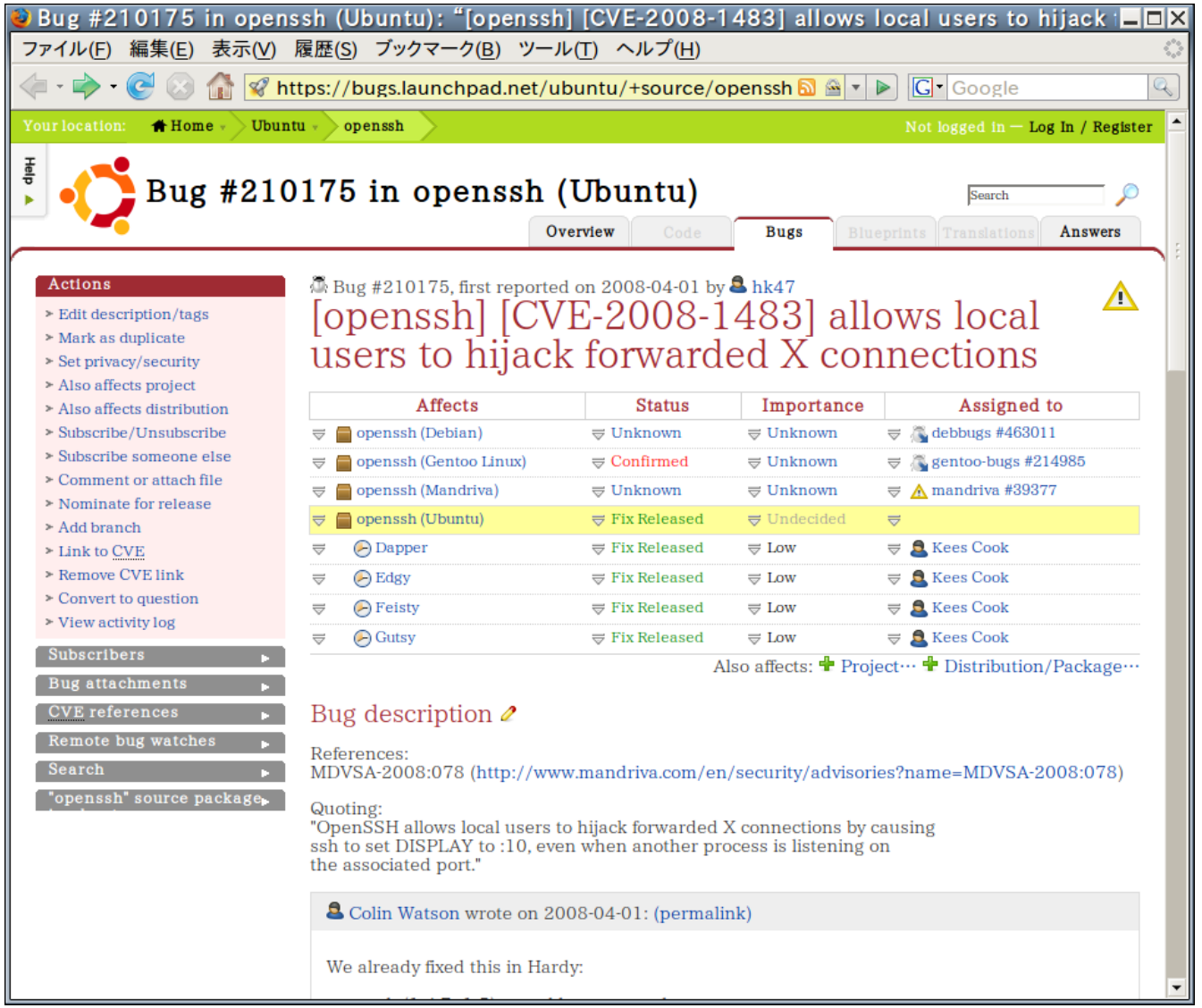


Ubuntu Bug Report

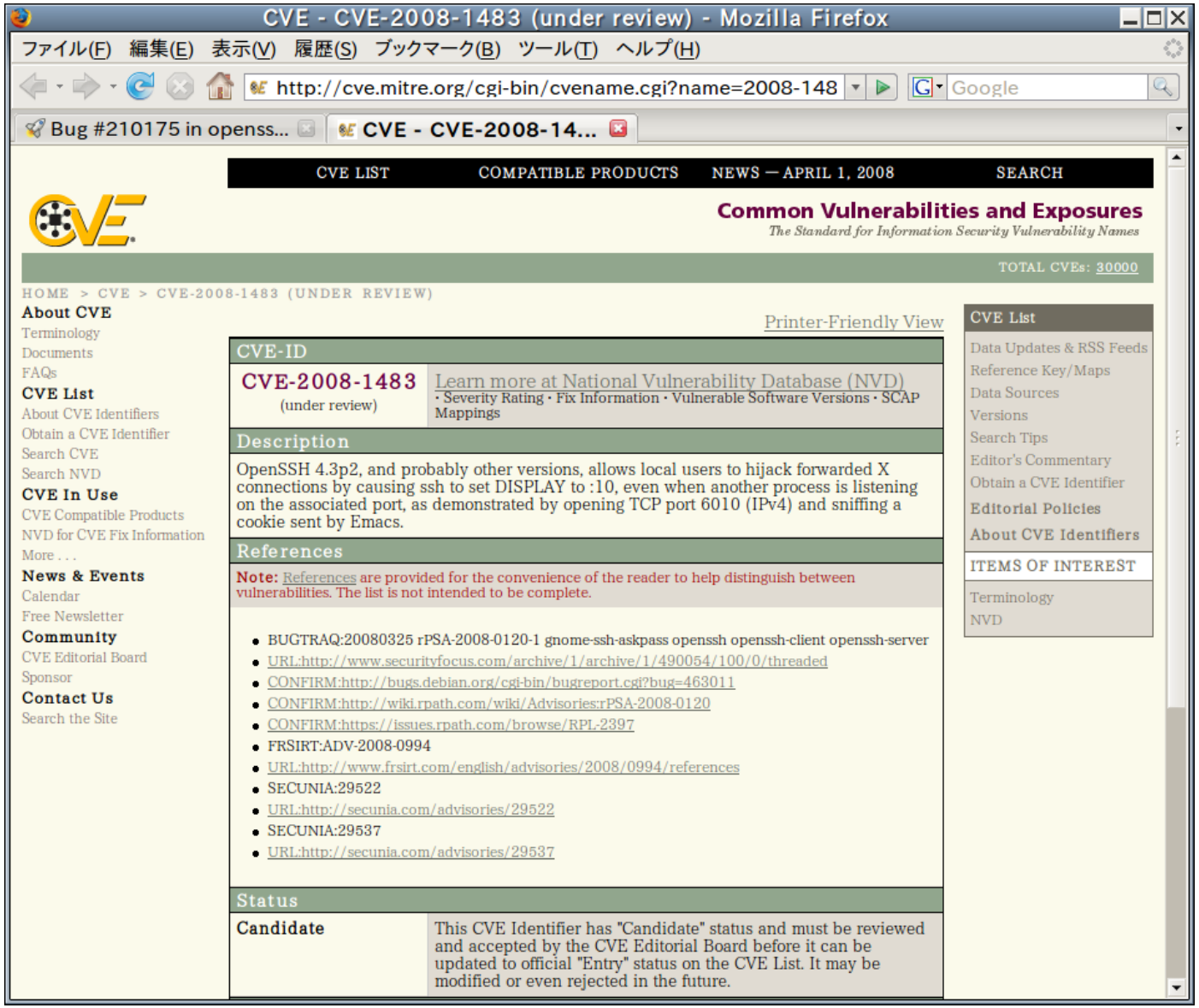
CVE-2008-1483



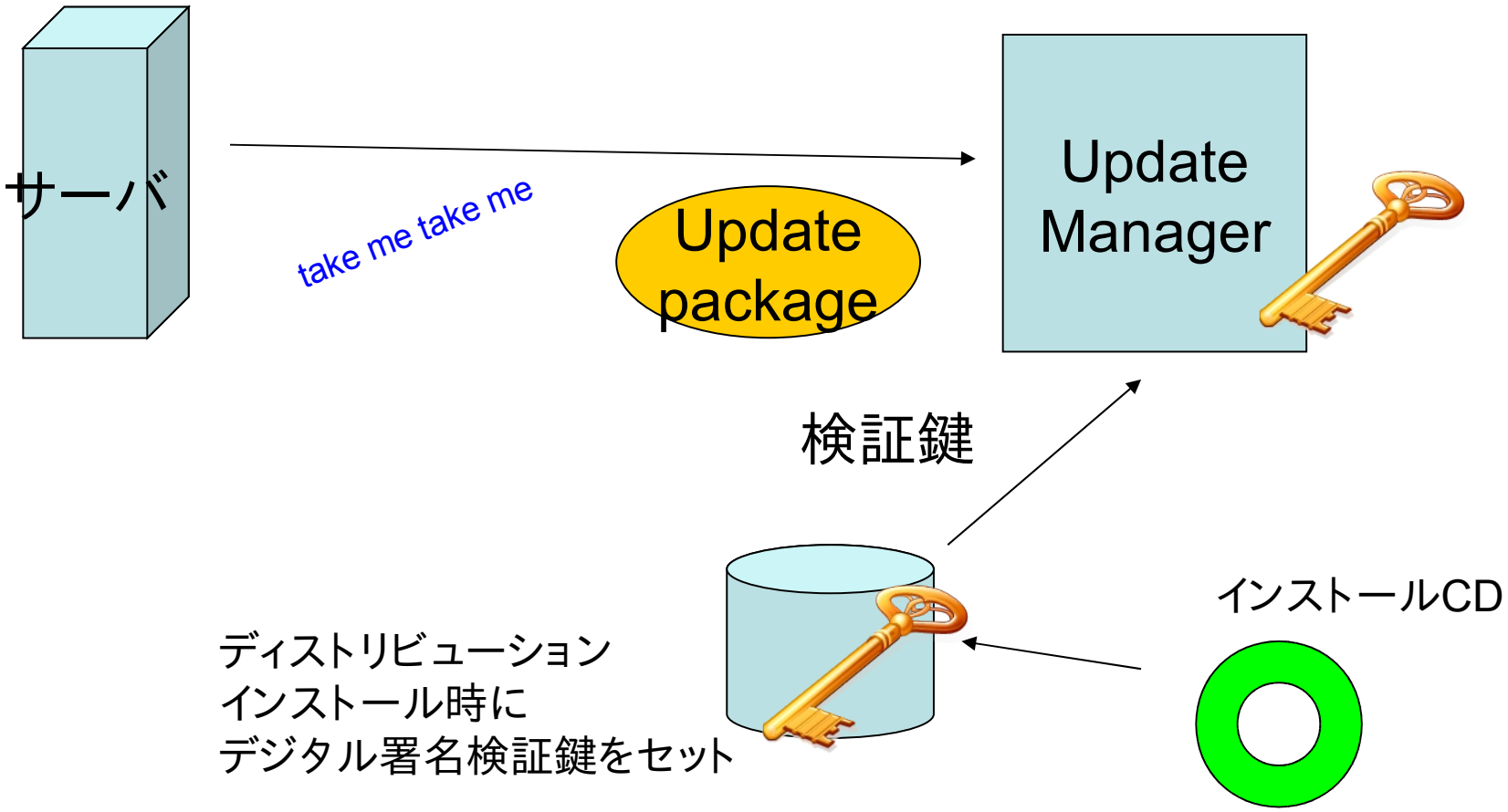
Ubuntu Bug Report



CVE

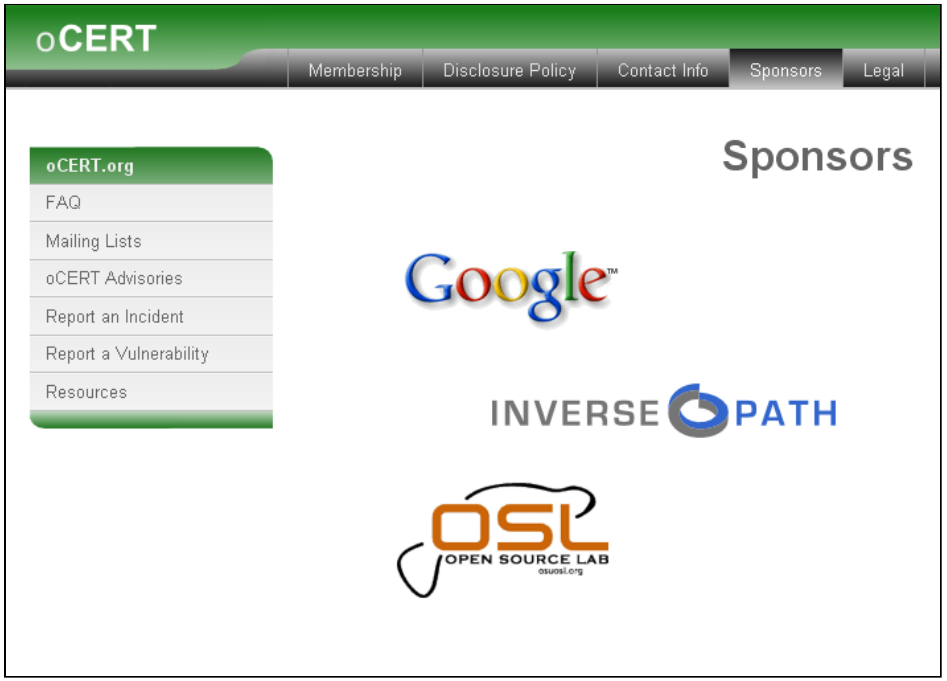

CVE - CVE-2008-1483 (under review) - Mozilla Firefox
ファイル(F) 編集(E) 表示(V) 履歴(S) ブックマーク(B) ツール(T) ヘルプ(H)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=2008-148
Google
Bug #210175 in openss...
CVE - CVE-2008-14...
CVE LIST
COMPATIBLE PRODUCTS
NEWS — APRIL 1, 2008
SEARCH
Common Vulnerabilities and Exposures
The Standard for Information Security Vulnerability Names
TOTAL CVEs: 30000
HOME > CVE > CVE-2008-1483 (UNDER REVIEW)
About CVE
Terminology
Documents
FAQs
CVE List
About CVE Identifiers
Obtain a CVE Identifier
Search CVE
Search NVD
CVE In Use
CVE Compatible Products
NVD for CVE Fix Information
More . . .
News & Events
Calendar
Free Newsletter
Community
CVE Editorial Board
Sponsor
Contact Us
Search the Site
Printer-Friendly View
CVE-ID
CVE-2008-1483
(under review)
Learn more at National Vulnerability Database (NVD)
• Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings
Description
OpenSSH 4.3p2, and probably other versions, allows local users to hijack forwarded X connections by causing ssh to set DISPLAY to :10, even when another process is listening on the associated port, as demonstrated by opening TCP port 6010 (IPv4) and sniffing a cookie sent by Emacs.
References
Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.
BUGTRAQ:20080325 rPSA-2008-0120-1 gnome-ssh-askpass openssh openssh-client openssh-server
URL:http://www.securityfocus.com/archive/1/archive/1/490054/100/0/threaded
CONFIRM:http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=463011
CONFIRM:http://wiki.rpath.com/wiki/Advisories:rPSA-2008-0120
CONFIRM:https://issues.rpath.com/browse/RPL-2397
FRSIRT:ADV-2008-0994
URL:http://www.frsirt.com/english/advisories/2008/0994/references
SECUNIA:29522
URL:http://secunia.com/advisories/29522
SECUNIA:29537
URL:http://secunia.com/advisories/29537
Status
Candidate
This CVE Identifier has "Candidate" status and must be reviewed and accepted by the CVE Editorial Board before it can be updated to official "Entry" status on the CVE List. It may be modified or even rejected in the future.
CVE List
Data Updates & RSS Feeds
Reference Key/Maps
Data Sources
Versions
Search Tips
Editor's Commentary
Obtain a CVE Identifier
Editorial Policies
About CVE Identifiers
ITEMS OF INTEREST
Terminology
NVD

デジタル署名でパッケージの正当性の確認



oCERT

- oCERT
  - Open Source 専用のCSIRTチーム



GNU/Linux and Government

SecretSecret

- Security-Enhanced Linux
  - the National Security Agency
- the Composable High Assurance Trusted Systems (CHATS)
  - the Defense Advanced Research Projects Agency

Conclusion

- ディストリビューションのセキュリティアップデートは便利である
- メジャーなディストリビューションやアプリケーションコミュニティは、組織化され、処理プロセスは明確である
- フリーソフトウェア間の生存競争は激しく、常にアルタナティブが存在しているためセキュリティ対応も速い
- フリーソフトウェアも商用ソフトウェアとまったく同じ脆弱性流通のプロセスを行っている
- 米国政府では予算をとりフリーソフトウェア・オープンソースの安全性向上に取り組んでいる

Question?

Happy Hacking!!