TechStyle

Linux Conference 2002

インターネットアプリケーションにおける オープンソースシステムのセキュリティ確保

岡田 良太郎

株式会社テックスタイル
104 0045
東京都中央区築地2ー1ー14**トミービル**5F
03 5148 5019 / fax 03 5148 0114
http://techstyle.jp/
info@techstyle.jp

September, 2002

TechStyle

- はじめに

- Linux **は**Linus Torvalds **の米国およびその他の国におけるの登録商標あるいは商標です。**
- X Window System **は、**X Consortium, Inc.**の商標です。**
- Red Hat **は、米国** Red Hat Software, Inc. **の登録商標です。**
- **その他、記載されている会社名、製品名は各社の登録商標または商標です。**
- **本資料の著作権は岡田良太郎に帰属します。**

September, 2002

TechStyle

Agenda

**WEB 改ざん、クロスサイトスクリプティング、データ漏洩の問題が頻発する中、オープンソース基盤のアプリケーションは増大の一途をたどっている。
ベンダー保守や開発会社依存のできないオープンソースシステムにおいて、セキュリティ品質確保のために何ができるのか。最近のセキュリティ事情を中心に見据えながら、方針面、技術面における方策について説明する。**

- I 最近の事情について
  - インターネットサーバとオープンソースシステムインフラ
  - アップデート最新事情
  - セキュリティホールの原理の基礎
- II 具体的な方策
  - 品質確保の考え方
  - 被クラック調査
  - アップデートにまつわる事柄
- III Others…

TechStyle

インターネットサーバ

- WEB/Mailなどを中心としたサービス
  - ホスト数はいまだに急増
  - ネットワークインフラの進歩
- しかし、特異なサービスである
  - 「常時」： 想定以上の期待
  - 「不特定」:顔が見えない
- カンタンそうで難しい。
  - 「可用性」と「事業継続性」

セキュリティとは

「セキュリティ」

- (1) 安全。防犯。安全保障。
- (2) 〔有価〕証券。
  - - 大辞林より

「きわめて経営的な言葉であり、技術用語ではない。」

セキュリティ3要素

- 機密性：対象（人）、内容（データ）の関係を保証
- 完全性：情報発信側と情報受信側の正確な伝達
- 可用性：期待されるときはいつでも応じられる

これらは「責任」によって分類されたものである

セキュリティ3要素と目的（例）

	情報サービス	EC	銀行	コミュニティ
機密性	○	◎	◎	○
完全性	◎	○	◎	○
可用性	○	◎	○	○

セキュリティ3要素と脅威

- 機密性：対象（人）、内容（データ）の関係を保証
  - 顧客データ漏洩，　ID不正利用
- 完全性：情報発信側と情報受信側の正確な伝達
  - WEBサイト改ざん，ウイルス感染
- 可用性：期待されるときはいつでも応じられる
  - サーバダウン，タイムアウト

最新事情 – 重要なアップデート

- Samba(2002/6/19)
- Apache (2002/6/20)
- Sendmail(2002/6/25)
- OpenSSH(2002/6/26)
- Resolver(2002/7/10)
- OpenSSL(2002/7/30)
- PHP(2002/9/6)
- OpenSSL Slapper Worm(2002/9/14)

…

Apache

- **対象**:Apache1.2**全バージョン**、Apache1.3〜1.3.24、Apache2.0〜2.0.36
- **原因**: chunked encoding**コードに脆弱性**
- **影響**:Apache Web**サイト全てに影響**
- **脅威**:**サービス停止**
- **種別**:DoS(**denial of service attack**)

TechStyle

chunked encodingとは

「ABCDEFGHIJKLMNOPQRSTUVWXYZ」という文字列を送る場合

chunked encoding しない場合

```
各種ヘッダ
各種ヘッダ
各種ヘッダ
Content-Length: 26

ABCDEFGHIJKLMNOPQRSTUVWXYZ
```

chunked encoding の場合

```
各種ヘッダ
各種ヘッダ
各種ヘッダ
Transfer-Encoding: chunked

0a  ←バイト数
ABCDEFGHIJ
0a
KLMNOPQRST
06
UVWXYZ
0
```


TechStyle

Slapper Worm

- OpenSSLの脆弱性をつくWorm(2002/9/14)
  対象：ApacheとApache-SSLを動作させているWEBサーバ
  - Apacheのバージョンをチェック
    - OpenSSLのバージョンと動作状況を確認
  - OpenSSLのセキュリティホール(0.9.6d以前)
    - ソースコード(/tmp/.bugtraq.c, /tmp/.bugtraq)を送り込む
    - コンパイルしてしまう
    - 常駐して2002番ポートから通信を開始

調査部分と侵入路が異なる顕著な例

Apache対応のおさらい

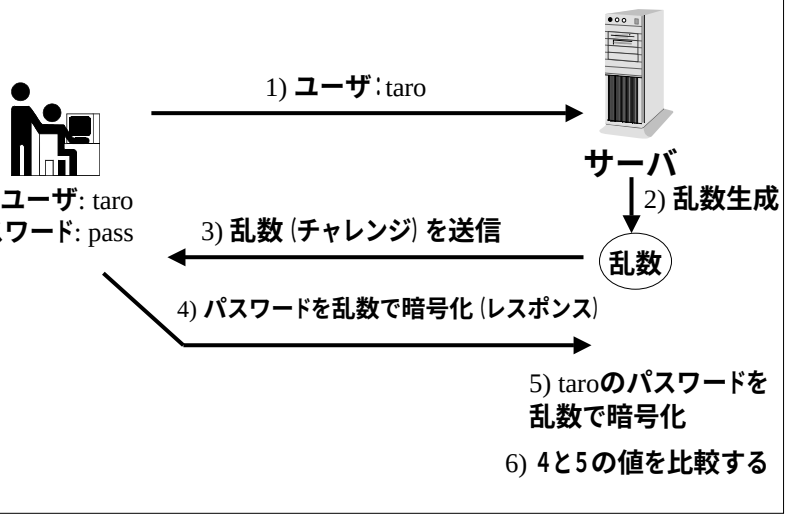
- 1.3.26あるいは2.0.39にアップグレード（推奨）
  - 主要なディストリビューションはリリースしている。
- このさいApache 2へ移行計画を
  （テスト環境の構築にそろそろ意味がでてきた）
- 1.3.26あるいは2.0.40にアップグレード
  - Upgrade your Apache HTTP Server to version 1.3.26 or 2.0.40 or higher. (Unix systems are safe at version 2.0.39.) - httpd.apache.org
- URL:http://httpd.apache.org/

OpenSSH

- 対象:OpenSSH 2.3.1p1〜3.3
- 影響:ssh2によるリモート運用管理に影響
- 原因:チャレンジ･レスポンスコードに脆弱性
- 種別:バッファオーバーフロー
- 脅威:リモートから任意のコードを実行
- 対処:3.4にアップグレードあるいは設定変更
- URL:http://www.openssh.org/

TechStyle

チャレンジ･レスポンス認証とは



TechStyle

OpenSSH対応のおさらい

- 3.4にアップグレードあるいはパッチ適用（推奨）
  - *BSD, Debian, Miracle Linuxなどはリリースしている。
  - RHはデフォルトで下記の設定が組み込まれていないので現状では問題ないらしい
- sshd_configで設定変更（短期的にOK）

  ChallengeResponseAuthentication no
  PAMAuthenticationViaKbdInt no

  あるいは3.3以降デフォルトになっている**UsePrivilegeSeparation** の利用

名前解決 - DNS Service

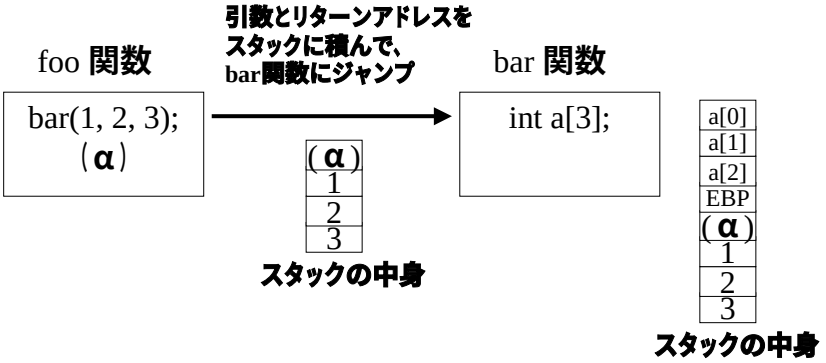
- 実は最も深刻な被害を出す可能性のあるサービス
- 設定終了時に忘れられるサービス
- Ping/telnet/ssh の障害でも気づかれないこともある
- ネットの不具合でも影響を受ける
- わかりやすく言えば、URLやドメインが脅威にさらされる

「いいWEBサイト作っても、ドメインごと乗っ取られてどうする」

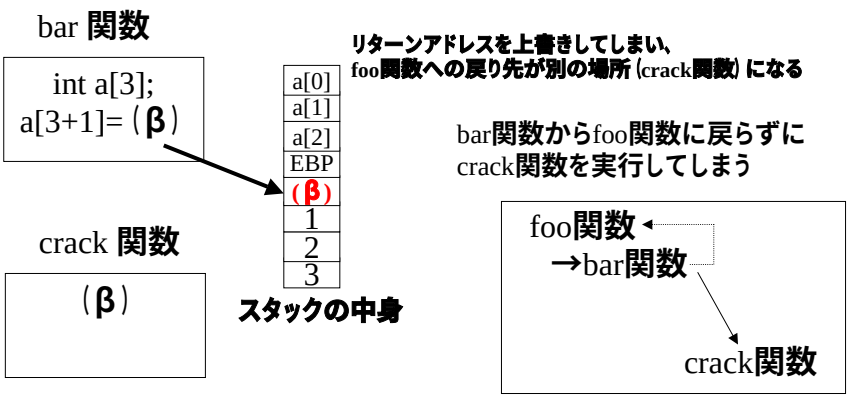
Resolver

- DNSの名前解決エンジン部分
- 対象:BSD resolverルーチン(libc)を使用する全アプリケーション
- 原因:Resolverライブラリコードに脆弱性
- 影響:BSD系OSのみ（FreeBSD/OpenBSD/NetBSD）に影響
- 脅威:サービス停止
- 種別:DoS(denial of service attack）
- 対処:アップグレード

バッファオーバーフローとは(1/4)



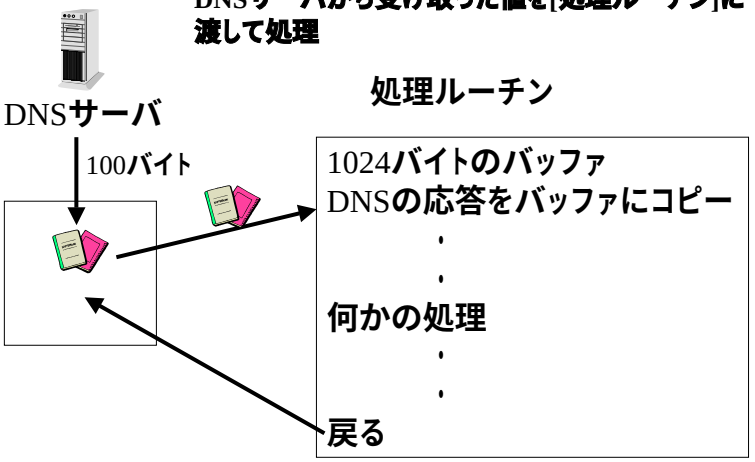
バッファオーバーフローとは(2/4)



TechStyle

バッファオーバーフローとは(3/4)

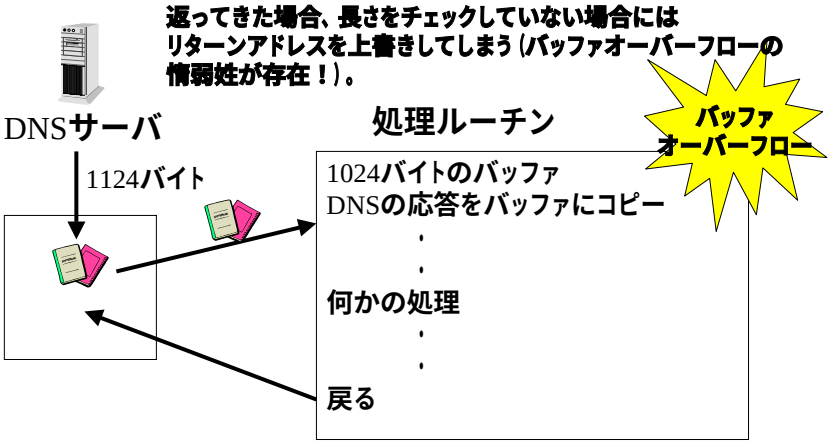
DNSサーバから受け取った値を[処理ルーチン]に渡して処理



TechStyle

バッファオーバーフローとは(4/4)

[処理ルーチン]で想定している長さ以上の値がDNSから返ってきた場合、長さをチェックしていない場合にはリターンアドレスを上書きしてしまう（バッファオーバーフローの脆弱性が存在！）。



バッファオーバーフロー対策

- 最新版にアップグレード
- StackGuardを利用する
  (http://www.cse.ogi.edu/DISC/projects/immunix/StackGuard/)
- libsafeを利用する
  (http://www.avayalabs.com/project/libsafe/index.html)

StackGuardは各アプリケーションを再コンパイルする必要がある。
libsafeは導入するだけでOK

Resolver対応のおさらい

- BSD系OSのみ（FreeBSD/OpenBSD/NetBSD）はパッチがリリースされている
  - Dynamicリンクで使用しているソフトはrestartすれば良い
  - Staticリンクで使用しているソフトはソースからすべて再コンパイルする必要がある

    http://www.cert.org/advisories/CA-2002-19.html

- glibc2.1.2とそれ以降は関係ない模様。
  http://www.kb.cert.org/vuls/id/AAMN-5BMSW2

  ただ、組み込みも可能なので、自前で作っているものがあれば要チェック

Sendmail

- **対象**:8.12.0〜8.14.4
- **原因**:**バッファオーバーフロー**
  - TXT**レコードの内容により**DNS**マップを行う設定になっている場合**
- **対策**:
  - 8.12.5**にアップグレード**
  - TXT**レコードを読み込まないようにする**
- http://www.kb.cert.org/vuls/id/814627
- http://www.sendmail.org/

Samba

- **対象**:Samba 2.2.3 **以前**
  - **（**--with-tdbsam**オプションが指定された場合のみ）デフォルトでは指定されていない**
- **バッファオーバーフロー**
  - SAM **の格納先として** tdb **を利用した場合に、**smb.conf **から変数を読み込む際のルーチン**
- **対策**:
  - 2.2.5/2.2.4-ja-1.0**にアップグレード**
  - --with-tdbsam**オプションを利用しない**
- http://www.samba.gr.jp/news-release/2002/20020703-1.html

TechStyle

セキュリティ対応

- セキュリティ対応のための重要なファクタ
  - 事象・原理に関する知識
  - ソフトウエア入手の確保
  - 実行動作環境
  - ソフトウエア配布の手段
  - 検証環境・検証プロセス
  - 性能要件・機能要件
  - 情報源と問題把握
  - 予防体制・対応体制

  …

TechStyle

後半へつづく

Please feel free to mail me
riotaro@techstyle.jp