WindowsとLinuxのセキュリティ: 2003

小島 肇　龍谷大学理工学部
kjm@rins.ryukoku.ac.jp

◆鑑賞上の注意

- タイトルに◆マークがあるページは、みなさんお手持ちのハンズアウトにはありません。
  - たとえばこのページ
- その他、適宜情報をアップデートしてある部分があります。
- このプレゼンテーション資料は http://www.st.ryukoku.ac.jp/~kjm/security/ で公開されます。

今日のお話

- 欠陥報告に見る Windows と Linux のセキュリティ
- Slammer と Blaster: Linux で発生する可能性
- Windows から Linux へ移行すればより安全になるのか?
- OS の区別の意味がない領域について

欠陥報告に見る Windows と Linux のセキュリティ

Part 1:
Windows の場合

Microsoft: 2003.01.01-10.06

- MS03-001~MS03-040
  - 緊急: 17
  - 重要: 17
  - 警告: 5
  - 注意: 1
- Microsoft セキュリティ修正プログラム管理ガイドでの推奨適用期限は……
  http://www.microsoft.com/japan/technet/security/topics/patch/secpatch/
  - 緊急: 24h 以内
  - 重要: 1 か月以内
  - 警告: 4 か月以内
  - 注意: 1 年以内

緊急: 17 の意味

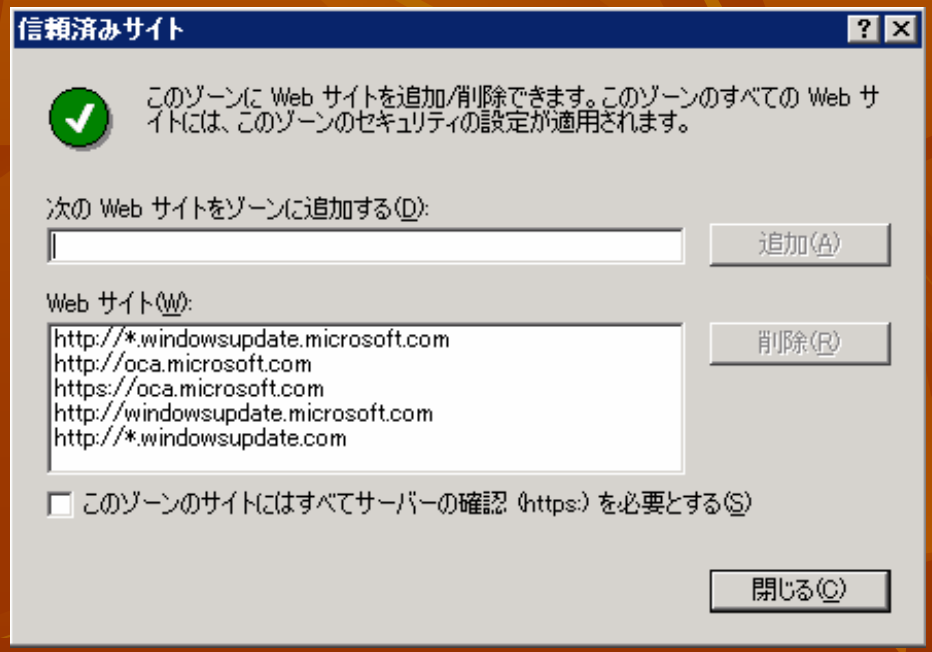
- 少なくとも 17 回は再起動が必要
  - Windows 2000 Server: 13 回
    OS: 7 + IE: 5 + Java VM: 1
  - IE の修正プログラムで再起動させられるのは納得できない
- 24h 以内の対応を推奨する、が 17 回
  - 現実には、特にサーバ系を 24h 以内に対応させるのは困難だと考えられる…
  - テスト環境に即座に適用し、機能テスト + ストレステスト (24h～72h) 後本番環境に適用?
  - 運用者による対応ポリシーの明確化が必要

緊急: IE: 5 の意味

- IE の欠陥はまず間違いなく「緊急」
  - 2003 年は全て緊急
  - 実は 2002 年も全て緊急(「緊急」と「高」)
  - 直ってない欠陥が待ち行列をなしている
    http://www.pivx.com/larholm/unpatched/
  - どこかに根本的な問題があるとしか思えない
- 修正プログラム適用後、なぜ再起動が必要なのか
  - 単なるアプリになってほしい。
  - OS とは分離してほしい。
- 迷惑。

緊急: IE: 5 の意味(続)

- Microsoft 的回答: **Internet Explorer 6 for Windows Server 2003**
  - セキュリティ強化の構成を実施
    http://www.microsoft.com/downloads/details.aspx?FamilyID=d41b036c-e2e1-4960-99bb-9757f7e9e31b&DisplayLang=en
  - 「緊急」が「警告」に



修正プログラムを適用したくない理由

- 再起動が必要
  - 特にサーバの場合
  - 予期できないスケジュールで発生するのでなおさら
- 副作用があることがある
  - 事例: MS03-032（XP + ASP.NET 1.0）、MS03-004（Outlook Express）
- テストが大変
  - 自動化は必須?

修正プログラムを適用したくない理由（続）

- 再起動後、管理者ログオンが必要になる場合がある
  - 事例: MS03-040（Windows NT 4.0 / 2000 + IE 5.01 / 5.5）
  - IE 6 にしましょう
- しかし適用しなくていいわけではない
  - 設定などで回避できる場合でも、いつかは適用しておいた方がいい
  - これらに対応したシステムを構築する必要がある

修正プログラムを（なるべく）適用しなくてもいいシステム

- あらかじめセキュアにしておく
  - 不要なサービス・ポートは閉じる: ICF、RRAS / IPsec フィルタ
    - やりすぎるとアプリが動かなくなるので注意
  - デフォルトではゆるい設定をセキュア側に: OS, IE、IIS、…
  - セキュリティ向上ハード・ソフトの導入
    - Firewall（境界、パーソナル、アプリケーション）
    - IDS（NIDS, HIDS）
    - アンチウィルス（ホスト、サーバ、メール・グループウェア）
  - 監査
    - File Integrity Check, log check
    - Computer Forensic
- しかし適用しなくていいわけではない
  - 特にアンチウィルスへの過信は禁物

修正プログラムを適用できないシステム

- セキュリティ hotfix が終了しているシステム
  - Windows NT 4.0 Workstation
  - Windows 95 / 98 / 98SE
- 早急なリプレースが必要、だが…
  - サポートが終了されていることに気がついていない人がいる
  - 欠陥がないことと、欠陥の存在が調べられていないことの区別のつかない人がいる
  - わかっちゃいるけどやめられない人がいる
    - お金…

修正プログラムの適用

- 適用手段
  - 個別の hotfix を手動で適用
    - 適用状況の検証: HFNetChk / MBSA
  - pull 型
    - Windows Update による適用
    - 自動更新 / Software Update Service による適用
  - push 型
    - SMS による適用
    - 3rd party 製品を利用した適用
    - Windows 標準機能を利用してがんばる適用

◆Microsoft 的回答: 2003.10.09

- マイクロソフト、現行のセキュリティ対策に追加して、新たな強化策を発表
  http://www.microsoft.com/japan/presspass/detail.aspx?newsid=1729
- 修正プログラムは原則として月刊制に
  - 第二火曜日（米国時間）
    - 修正プログラムの適用をスケジューリング可能
    - 総テスト回数を減らすことが可能
  - 必要に応じて緊急出版の可能性あり

◆ Microsoft 的回答: 2003.10.09（続）

- サポート延長: 2004.06 まで
  - Windows NT 4.0 Workstation
  - Windows 2000 SP2
- 機能向上
  - Windows XP SP2 / Server 2003 SP1
  - SUS 2.0（2004 前半）
- その他
  - 教育プログラム

◆ Microsoft 的回答: 2003.10.09（続）

- 月刊 Windows Update: 2003.10
  - Windows: 5 件
  - Exchange: 2 件

	Me	NT	2000	XP	2003
MS03-041	○	×	×	×	△
MS03-042	○	○	×	○	○
MS03-043	○	×	×	×	△
MS03-044	△	△	△	×	×
MS03-045	○	△	×	△	△

MS03-045 でさっそく出しなおし事件発生…課題を残した

どのくらい待てるか

- MS03-026（Blaster）:
  - 公開: 2003.07.17（木曜日）
  - 攻略プログラム登場: 2003.07.21
  - 時間差: 4 日
- MS03-040（MS03-032 直し忘れ）:
  - 公開: 2003.10.04（土曜日）
  - 攻略プログラム登場: 2003.09.07
  - 時間差: -28 日

どのくらい待てるか（続）

- 緊急対応として、機能を低下させてでも回避策を採らなくてはならない場合がある
  - IE の場合はたいてい JavaScript や ActiveX の無効化
  - まともにナビゲートできないサイトが続出する
- 土日や祝祭日、長期休暇中に修正プログラムが公開されることも考えられる
  - あるいは攻略プログラムが
  - 対応ポリシーの検討・策定が必要

Part 2:
Red Hat Linux の場合

なぜ Red Hat?

- 今のところ、広く利用されている
- 熱心にセキュリティ fix を出しているように見える
- Debian GNU/Linux はパッケージ多すぎ ^^;;

Red Hat Linux: 2003.01.01-10.06

- 実質上 104 個の新規修正パッケージ
  - 内容的に重複するものは排除
  - 番号更新版（例: RHSA-2003:256-01 から RHSA-2003:256-02）の場合は、新しい内容が含まれていれば新規と数えた
- 出しなおし、が散見される
  - 例: RHSA-2003:256-02 Updated Perl packages fix security issues.
    Added updated mod_perl packages for Red Hat Linux 7.1, which are required due to the move to Perl version 5.6.1 on this platform.
  - 元プロダクトが何度も出しなおす例も: OpenSSH

深刻度の評価

- Red Hat Linux は深刻度を表記していない
  - 各自で深刻度を判断する必要があるが、Red Hat Errata は日本語化さえロクにされていない。利用者はこれで本当に深刻度を判定できているのか?
    - Red Hat Enterprise Linux 用のページは日本語化されているようだ…そんなレベルで差別化するとはね
    - もちろん Windows の場合も最終的には各自で判断するのだが、Microsoft による深刻度判定が目安として使えるのは大きい
    - にもかかわらず、米国では「わかりづらい」として訴訟に発展しているという事実
  - 開発元の情報を参照したり、オープンソースの利点を利用してソースの差分を参照したりもできるが、一定以上のスキルが必要になる。

OS の再起動が必要になるのは...

- Kernel, 基幹 library（glibc）の更新
  - Kernel: 6
  - glibc: 1
- 各モジュールの更新では OS の再起動までは不要
  - 各モジュールに関連する要素を再起動
    例: OpenSSL を更新したら、OpenSSL を利用しているモジュールは再起動した方がよいだろう

修正プログラムを適用できないシステム

- サポートが終了しているシステム
  - Red Hat Linux 6.2 / 7.0
- Use the source, Luke!
  - 他ベンダー提供の保守サービスを使う
    例: Red Hat Linux アップデートサービス（テンアートニ）
    http://www.10art-ni.co.jp/service/rh_update/index.html
  - 自力でがんばって保守する
  - 他のディストリビューション / Free UNIX に乗り換える

修正プログラムを適用できないシステム（続）

- Red Hat Linux 7.1～8.0 は今年いっぱい
- Red Hat Linux 9 は 2004.04.30 まで（あと半年）
- Red Hat Enterprise Linux は原則 5 年サポートされるようです。
- 今後の Red Hat Linux は、コミュニティベースにより開発される Fedora Project 版と、これまでと同様の Red Hat Enterprise Linux の 2 本立てになるようです。
- どうするのか、今のうちに考えておきましょう。

修正プログラムの適用

- 適用手段
  - 個別の修正パッケージを手動で適用
    - rpm –Fvh package….
  - pull 型
    - up2date による適用
    - Red Hat Network への登録が必要
  - push 型
    - ssh などのリモート管理機構 + rpm を利用

up2date の楽しい話題

- up2date に組み込まれた SSL 証明書が 2003.08.10 に失効
- これに対応するため、更新版の up2date パッケージを 2002.10 / 2003.05 に配布していた
- が、この更新版 up2date の SSL 証明書は 2003.08.28 に失効!
- 失効後に(!!) up2date の再更新版が登場して今に至る。
  http://www.redhat.co.jp/products/rhn_info.html
- Red Hat だいじょうぶか?

◆どのくらい待てるか

- ProFTPD ASCII File Remote Compromise Vulnerability
  http://xforce.iss.net/xforce/alerts/id/154
  - 公開: 2003.09.24（水曜日）
  - 攻略プログラム登場: 2003.10.14
  - 時間差: 20 日
- lsh 1.4 remote root exploit
  http://lists.netsys.com/pipermail/full-disclosure/2003-September/010489.html
  - 公開: 2003.09.20（土曜日）
  - 攻略プログラム登場: 2003.09.19
  - 時間差: -1 日

◆どのくらい待てるか（続）

- Solaris 2.6～9 sadmind remote root exploit
  http://archives.neohapsis.com/archives/vulnwatch/2003-q3/0109.html
  - 公開: 2003.09.16（火曜日）by iDefense / Sun
  - 攻略プログラム登場: 2003.08.26
  - 時間差: -20 日
- GNU FTP Server (ftp.gnu.org) compromized
  http://www.cert.org/advisories/CA-2003-21.html
  - 公開: 2003.08.13（水曜日）
  - 占拠されたのは: 2003.03～07
  - 時間差: 150 日?!

Part 3:
いくばくかの項目

いつもの顔ぶれ

- Windows
  - IE (5)
  - Java VM (1)（2004.09.30 でサポート終了）
  - IIS (1)
  - Media Player (2)
  - MS Office (5)
  - SQL Server (1)

いつもの顔ぶれ

- Linux
  - kernel (6)
  - sendmail (4)
  - OpenSSL (3)
  - OpenSSH (3)
  - Apache, PHP (6)
  - XFree86, KDE (5)

いつもの顔ぶれの特徴

- 複雑
- 機能がたくさん
- 機能が日々追加される

…つまり、

- 安定し得ない?

対極

- djb tools (http://cr.yp.to)
  - qmail
  - djbdns
  - publicfile
- 単純
- 単機能コマンドを組み合わせて使う
- 機能を増やさない
- 必要とあらば互換性を捨てる、プロトコルを変える

2003 年はおとなしかった顔ぶれ

- Linux
  - bind（新規ものはない）
- 出尽くした?
  - まだまだ要注意だよねえ

Slammer と Blaster: Linux で発生する可能性

Slammer のおさらい

- 欠陥: SQL Server 2000 解決サービスのバッファのオーバーランにより、コードが実行される (323875) (MS02-039)
- 対象: SQL Server 2000 / Microsoft Desktop Engine 2000（MSDE 2000）
- 1434/UDP を利用して攻撃・拡散
  - コネクションレスなのでむやみやたらに送りつけることが可能 → 高速な拡散
  - オン・メモリなので、メモリの検査のできないアンチウィルスソフトには見つからない

Slammer のおさらい（続）

- 驚くほど多くのソフトウェアが SQL Server / MSDE を利用
  - 気がつかないまま利用 → ヤラレ
  - Microsoft を含め、利用状況を把握していなかったベンダーは多い。いわんやユーザーをや。
- 修正プログラムの適用も簡単ではなかった
  - 当初公開されていたのは、インストーラ型ではなく、いくつもの導入手順の必要な、複雑なものだった

Linux でもあり得るか?

- UDP を利用した攻撃が可能な欠陥が、多くのシステムに共通して存在すれば、原理的には可能だと思われ
- そのようなソフトの例: DNS server
  - bind – いろいろ話題を振りまいた
  - djbdns – 安全性では定評がある
- bind 方面は、今年に入ってからは落ち着いているようだが…
- 2001 年の li0n worm がもっと洗練されていれば、…
- メモリの検査のできるような Linux 用アンチウィルスソフトはあるのか?

Blaster のおさらい

- 欠陥:RPC インターフェイスのバッファ オーバーランによりコードが実行される (823980) (MS03-026)
- 対象: Windows NT 4.0 / 2000 / XP / Server 2003
  Blaster の直接の対象は Windows 2000 / XP
- 135/TCP を利用して攻撃・拡散
- 対象機器がとんでもなく多い
  - Code Red, Slammer: 数十万台
  - Blaster: 数千万～数億
- 教訓
  - クライアントへの修正プログラム適用の必要性
  - デフォルト設定でのセキュリティ確保の重要性

Linux でもあり得るか?

- 最近の Linux / PC UNIX はかなりデフォルトセキュアになってきている
  - が、意外に穴穴なディストリもあるので注意しよう
- たとえば Red Hat Linux 9 のデフォルトデスクトップ環境では、外部から攻略可能なポートすらほとんどない
- 今後ともセキュリティを推進しておけば、Blaster ほどひどいことにはならないと考えられる
  - が、イントラ向けにいろいろサービスを起動すれば、それに比例して穴穴になるので注意しよう

Windows から Linux へ移行すればより安全になるのか?

いきなり結論

- 少なくとも現状では、以下の効果がある。
  - Windows / IE / Outlook, Outlook Express / MS Office 向けウィルスはたいてい無視できる
  - Windows / IE / Outlook, Outlook Express / MS Office向けの攻撃はたいてい無視できる
  - OS の再起動回数が低下
  - この効果はバカにできない
- 以下については効果は薄いかもしれない。
  - 詐欺的手法を用いた攻撃（spam, phishing, …）

いきなり結論（続）

- 以下については逆に対象になってしまう。
  - Linux を対象とした攻撃
  - 修正パッケージの適用頻度も上昇する
- 以下については低下してしまう。
  - セキュリティ情報・欠陥情報の日本語による提供
  - コミュニティへの参加、ソースの活用によりカバーできる可能性がある
  - UNIX は自ら助くる者を助く
  - ねだるな、あたえて、かちとれ（神林長平「ラーゼフォン 時間調律師」）

より効果を高めるには?

- 多様性はよいことだ（morris worm の教訓）
  - CPU: x86 系ばかりでなく、…
  - OS: 複数の OS、複数のディストリビューション、…
  - アプリケーション: web ブラウザ / http サーバ、メールクライアント・サーバ、…
- ただしメンテナンスコストは急激に増大
  - どこかでバランスを取る
  - 多様な環境をメンテナンスできないのなら「単一できっちり」の方がよい
  - 死守しなければならないものは何かを考える

Linux デスクトップが普及すれば...

- Linux 向けの攻撃は確実に増えると予想できる
  - 特に、一般ユーザを狙った攻撃が
  - サーバソフトウェアのコードについてそれなりに調べられてきているが、デスクトップ環境や web ブラウザについては、まだまだなのではないか?
- いわゆるセキュア OS の機能が使いやすく組み込まれるとうれしいかな
- IT Pro 向けだけでなく、ふつうの人でも理解できる情報をもっと提供していく必要がある
  - この観点では Microsoft の方が遥かに先行している(が、それでも不十分)
  - 人のフリ見て我がフリ直せ

◆OS の区別の意味がない領域について

◆ OS ベンダーが維持してくれないもの

- 独自構築アプリケーション / システム
  - 公開 web アプリケーション
  - データベース（の中身）
  - 社内システム
- 3rd party ソフトウェア: おうおうにして、まともに維持されていない…
- OS / ディストリビューションに含まれていない、オープンソース / フリーソフトウェア
- OS / ディストリビューションに見捨てられた、オープンソース / フリーソフトウェア

◆本当に重要なもの

- 独自の資産
  - 独自システム
  - 独自ノウハウ
  - データ
- OS ではない
  - 状況に応じて、必要に応じて、OS は選択して利用するものでありたい
  - 手間がかかるけど

おしまい

質問はありますか?