OSSIR
Groupe Sécurité Windows

Réunion du 7 mars 2005

Revue des dernières vulnérabilités Microsoft

Nicolas RUFF

nruff@security-labs.org

Dernières vulnérabilités
Avis Microsoft (1/6)

- **Avis de sécurité Microsoft depuis le 7 février 2005**
  - **MS05-004 : vulnérabilité dans la validation des chemins ASP.NET**
    - **Affecte : .NET Framework 1.0 et 1.1**
    - **Exploit : remplacer le caractère / par \ ou %5C permet de contourner les contrôles d'accès aux pages ".aspx" (déjà connu)**
    - **Crédit : N/D**
  - **MS05-005 : "buffer overflow" dans Office XP**
    - **Affecte : Office XP (uniquement)**
    - **Exploit : "buffer overflow" lorsque l'utilisateur clique sur une URL longue contenant :**
      - **http://www.myhost.com/myfile.doc%00aa...aa.doc**
      - **http://www.hhs.gov/ocr/privacysummary.rtf%0a"+mylongstring**
    - **Crédit : Rafel Ivgi / Finjan (exploit publié)**
  - **MS05-006 : "cross-site scripting" et spoofing d'adresse dans SharePoint**
    - **Affecte :**
      - **Windows SharePoint Services for Windows Server 2003**
      - **SharePoint Team Services**
    - **Exploit : N/D**
    - **Crédit : N/D**

Dernières vulnérabilités
Avis Microsoft (2/6)

- **MS05-007 : fuite d'information via un tube SMB**
  - **Affecte : Windows XP**
  - **Exploit :**
    - **Un utilisateur peut obtenir la liste des personnes connectées à un serveur SMB**
    - **Le problème est bien plus large et concerne la possibilité d'accéder à n'importe quel tube nommé à travers la connexion anonyme à un tube anonyme**
  - **Crédit : J.B. Marchand / HSC**

- **MS05-008 : exécution de code à travers un évènement "drag and drop"**
  - **Affecte : Windows 98, 2000, XP, 2003 (autres versions non supportées)**
  - **Exploit :**
    - **Exploitable dans une page Web**
    - **Requière une interaction utilisateur**
  - **Crédit : N/D**

- **MS05-009 : "buffer overflow" dans le traitement des PNG**
  - **Affecte : Messenger 5.0, 6.1, 6.2, Media Player 9 (sauf XP SP2), Windows 98/ME**
  - **Exploit : exécution de code à l'ouverture d'un fichier PNG**
  - **Crédit : Juliano Rizzo / Core ST (exploit publié)**

Dernières vulnérabilités
Avis Microsoft (3/6)

- MS05-010 : "buffer overflow" dans le "license logging service"
  - Affecte : Windows NT4 Server, 2000 Server, 2003
  - Exploit :
    - "buffer overflow" exploitable à distance pour obtenir les droits SYSTEM
    - Basé sur le service LLSSRV.EXE et le tube LLSSRV
  - Crédit : Kostya Kortchinsky / CERT Renater

- MS05-011 : "buffer overflow" dans le driver SMB
  - Affecte : Windows 2000, XP, 2003
  - Exploit :
    - Les réponses FIND_FIRST2 et QUERY_FILE_INFORMATION n'acceptent pas plus de 116 octets
    - La vulnérabilité se produit en mode noyau (!)
    - Attaque baptisée "GreenApple" par Immunity
  - Crédit : eEye

Dernières vulnérabilités
Avis Microsoft (4/6)

- MS05-012 : vulnérabilités multiples OLE/COM
  - Affecte : Windows 2000, XP, 2003
    - Plus les applications utilisant OLE : Exchange 5.0, 5.5, 2000, 2003, Office XP, Office 2003
  - Exploit :
    - Élévation de privilèges via "COM structured storage"
    - Exécution de code via un objet OLE malformé
  - Crédit : Cesar Cerrudo / Application Security Inc.

- MS05-013 : exécution de code via l'ActiveX DHTML
  - Affecte : Windows 98/ME, 2000, XP, 2003
  - Exploit : le composant DHTML (dhtmled.ocx) permet d'injecter des scripts dans une autre page via execScript()
  - Crédit : N/D

Dernières vulnérabilités
Avis Microsoft (5/6)

- **MS05-014 : patch cumulatif pour IE**
  - **Affecte : IE 5.01, 5.5, 6.0**
  - **Exploit :**
    - **Vulnérabilité "drag and drop"**
    - **Spoofing dans le décodage d'URL par double encodage**
    - **"Heap overflow" dans le composant DHTML**
    - **"Cross domain scripting" via "Channel Definition Format" (CDF)**
  - **Crédit :**
    - **Michael Krax, Andreas Sandblad / Secunia**
    - **Jouko Pynnönen**
    - **Andreas Sandblad / Secunia**
    - **N/D**

- **MS05-015 : "buffer overflow" dans le traitement des liens hypertexte**
  - **Affecte : Windows 98/ME, 2000, XP, 2003**
  - **Exploit : la librairie "Hyperlink Object Library" contient un "buffer overflow" non spécifié**
  - **Crédit : Anna Hollingzworth**

Dernières vulnérabilités
Avis Microsoft (6/6)

- **Re-release**
  - **MS04-035 "Buffer overflow" dans le service SMTP**
    - **Version 1.2**
    - **Disponibilité d'un patch pour Exchange 2000 Server**
    - **Date initiale : 12 octobre 2004 …**
  - **MS05-005 Vulnérabilité dans Office XP**
    - **Version 1.3**
  - **MS05-006 Vulnérabilité SharePoint**
    - **Version 1.2**
    - **FrontPage 2002 n'est pas affecté**
  - **MS05-010 Vulnérabilité "License Logging Service"**
    - **Version 1.1**

- **Bulletins de sécurité pour le mois de mars : 0**
  - **Remarque : il y a souvent plus de bulletins les mois pairs que les mois impairs …**

Dernières vulnérabilités
Infos Microsoft (1/2)

- IE 7 sortira finalement fin 2005 (avant LongHorn)
  - Changement de cap face à l'explosion du "phising"
- Microsoft AntiSpyware restera gratuit
  - http://informationweek.securitypipeline.com/news/60401102
- Un point intéressant dans la licence MS AntiSpyware
  - Microsoft engage sa responsabilité à hauteur de $5 en cas de destruction de données
  - … intentionnelle ou non
  - http://news.zdnet.com/2100-1009_22-5590042.html
- "Les spywares, ces mouchards qui vous espionnent"
  - http://go.microsoft.com/?linkid=2110069
- "Ce que vous pouvez faire contre les logiciels espions et autres logiciels indésirables"
  - http://go.microsoft.com/?linkid=1852525
- Microsoft rachète Sybari (Antigen)
  - http://www.sybari.com/DesktopModules/PressReleases/PressReleasesView.aspx?TabID=0&Alias=Rainbow&Lang=en-US&ItemID=386&mid=10409

Dernières vulnérabilités
Infos Microsoft (2/2)

- Distribution automatique de XP SP2 par Windows Update fixée au 12 avril 2005
- Rights Management Services (RMS) Service Pack 1
  - Prévu cette année
  - Plus besoin d'Internet pour utiliser RMS
- ISA Server 2004 SP1
  - http://support.microsoft.com/?kbid=891024

- Outil MSRT
  - Un "Stinger"-like
    - La version "février 2005" recherche 12 virus
  - Mis à jour tous les mois avec les bulletins de sécurité
  - Distribué également par Windows Update
  - Nécessite d'être administrateur local
  - Envoie un rapport à Microsoft (!)

  - http://www.microsoft.com/security/malwareremove/default.mspx

  - Microsoft maintient une encyclopédie virale
    - http://www.microsoft.com/security/encyclopedia/details.aspx?name=Win32%2fZindos

Dernières vulnérabilités XP SP2 (1/1)

- **Un comportement curieux**
  - **Cliquer sur un lien dans OE6 SP2 n'ouvre pas IE**
  - **Par contre si IE est déjà lancé le lien est ouvert …**

Dernières vulnérabilités
Autres avis (1/3)

- **Sortie de FireFox 1.0.1**
  - Corrige le bogue "IDN" (entre autres)
- **"0-day" dans OWA permettant le phishing**
  - Redirection du login par une URL malformée
  - http://secunia.com/advisories/14144/
- **"0-day" dans la solution de sauvegarde BrightStor ARCServe**
  - Permet la prise de contrôle du serveur par envoi d'un paquet sur le port TCP/41523
  - http://archives.neohapsis.com/archives/bugtraq/2005-02/0123.html
- **Attaques ciblées par "DNS Cache Poisoning"**
  - Attaque dite "pharming"
  - Les produits Symantec sont particulièrement vulnérables
  - Source : SANS / ISC

Dernières vulnérabilités
Autres avis (2/3)

- La société Shavlik va faire son propre antispyware
  - Produit "NetChk Spyware"
  - Destiné aux administrateurs et non aux end-users
- Payer $34.95 par mois pour être désinscrit des listes de spammers ?
  - http://www.unsubscribenow.org/
  - L'imagination du marketing n'a pas de limite …
- Un remplacement OpenSource pour RIS : Unattended
  - http://unattended.sourceforge.net/
- Un remplaçant pour RunAs : SUperior SU
  - http://www.stefan-kuhr.de/supsu/main.php3
  - Des fonctions en plus (multi-desktop, etc.)

Dernières vulnérabilités
Autres avis (3/3) - virus

- Les antivirus Windows ne scannent pas les ".tgz"
  - http://zeedo.blogspot.com/2005/02/multiple-av-vendors-ignoring-targz.html
- Encore des problèmes avec les décompresseurs des antivirus
  - "Buffer overflow" dans le décompresseur ARJ de F-Secure
  - "Heap overflow" dans le décompresseur UPX de Symantec
- Un cheval de Troie s'attaque à l'anti-spyware de Microsoft
  - Nom de code : BankAsh.A / SpyBank
  - http://www.silicon.fr/getarticle.asp?ID=8497
- Alertes : MyDoom.BB, etc.

Questions / réponses

- **Questions / réponses**
- **Date de la prochaine réunion**
  - **Lundi 11 avril 2005**
- **N'hésitez pas à proposer des sujets et des salles**