OSSIR
Groupe Sécurité Windows

Réunion du 11 avril 2005

Revue des dernières vulnérabilités Microsoft

Nicolas RUFF

nicolas.ruff@eads.net

Dernières vulnérabilités
Avis Microsoft (1/3)

- **Avis de sécurité Microsoft depuis le 7 mars 2005**
  - **Pas de bulletins au mois de mars !**

- **Compléments d'informations**
  - **MS05-014 Patch cumulatif pour IE**
    - **"Heap Overflow" exploitable par la fonction JavaScript "createControlRange()"**
    - **Contournement des zones de sécurité avec un entête "Content-Disposition" malformé**
    - **Contournement des zones de sécurité avec un tag <OBJECT CODEBASE=…?.exe>**
    - **Crédit : Secunia**
  - **MS04-038 "Buffer overflow" dans le traitement des fichiers .CSS par IE**
    - **Exploit publié**

- **Re-releases**
  - **MS05-002 Vulnérabilités multiples dans le traitement des fichiers images**
    - **Version 1.2**
  - **MS05-004 Vulnérabilité dans le contrôle d'accès HTTP avec ASP.NET**
    - **Version 1.2**
  - **MS05-015 "Buffer overflow" dans l'objet "Hyperlink Object Library"**
    - **Version 1.2**

Dernières vulnérabilités
Avis Microsoft (2/3)

- **Le correctif MS05-002 n'est pas stable sur Windows 98/ME**

- **Remarque**
  - **MS05-010 est exploitable de manière anonyme sur Windows 2000 Advanced Server**
    - **http://www.immunitysec.com/downloads/llssrv_miss.pdf**

Dernières vulnérabilités
Avis Microsoft (3/3)

- **Prévisions pour le mois d'avril**
  - 5 bulletins Windows dont des "critiques"
  - 1 bulletin Office "critique"
  - 1 bulletin Messenger "critique"
  - 1 bulletin Exchange "critique"
  - 2 bulletins "non sécurité", "haute priorité" (???)

Dernières vulnérabilités Infos Microsoft (1/3)

- Nouveautés
  - ISA Server 2004 Standard SP1
  - ISA Server 2004 Enterprise
- Windows 2003 SP1 "officiel"
  - Des nouveautés au moins aussi profondes que XP SP2
  - Retour d'expérience plutôt positif
  - Mais également des problèmes …
    - Incompatibilité avec Dell OpenManage <= 4.2
      - http://www.dell.com/downloads/global/power/ps2q05-20050113-Callaway.pdf
    - Incompatibilité OWA
      - http://support.microsoft.com/kb/841561
- "Technology preview"
  - Indigo : la nouvelle API de communication universelle (.NET Framework 2.0)
  - Avalon : la nouvelle interface graphique unifiée
  - http://go.microsoft.com/?linkid=2575706

Dernières vulnérabilités Infos Microsoft (2/3)

- **Password Expiration Warning Application (PEWA)**
  - Prévient par mail les utilisateurs dont le mot de passe va expirer
  - http://support.microsoft.com/default.aspx?scid=kb;en-us;221977
- **Lutte antispam et antivirus ("Message Hygiene") chez Microsoft**
  - http://go.microsoft.com/?linkid=2575716
- **Quelques nouveaux sites MS (hors sécurité)**
  - Imaginons Demain
    - http://www.imaginonsdemain.fr/
  - Microsoft Class Server 3.0
    - http://www.microsoft.com/france/education/prim-sec/classserver/default.asp
- **Microsoft explique le "l33t speech"**
  - http://www.microsoft.com/athome/security/children/kidtalk.mspx

Dernières vulnérabilités
Infos Microsoft (3/3)

- Le gouvernement américain aura les patches un mois avant
  - http://www.reuters.com/newsArticle.jhtml?type=technologyNews&storyID=7876004&src=rss/technologyNews
- Microsoft change son fusil d'épaule sur les "0-day"
  - http://blogs.msdn.com/aaron_margosis/archive/2004/06/25/166039.aspx
  - "There have been a couple of credible sounding stories in the press in the past week or two about zero-day attacks - that is, the malicious exploitation of previously unknown vulnerabilities."
- Outil LimitLogin 1.0
  - http://download.microsoft.com/download/f/d/0/fd05def7-68a1-4f71-8546-25c359cc0842/limitlogin.exe
- Détecter les sniffers sur des machines Windows 2000+
  - Outil PromQry
  - Utilise WMI via RPC
  - http://support.microsoft.com/?kbid=892853

Dernières vulnérabilités
Autres avis (1/6)

- **Propagation du ver "CommWarrior" sur téléphones portables**
  - **Cible Symbian 60**
  - **Propagation par MMS (et BlueTooth)**
  - **Nécessite une confirmation utilisateur**

- **Verdict pénal dans l'affaire Guillermito/Tegam rendu le 8 mars**
  - **Guillermito a été reconnu coupable de "contrefaçon"**
  - **Condamné à 5000 euros d'amende avec sursis**
  - **Sans l'inscription au Bulletin n°2 du casier judiciaire**

  - **http://www.zdnet.fr/actualites/informatique/0,39040745,39210830,00.htm**
  - **http://solutions.journaldunet.com/0503/050309_guillermito.shtml**
  - **http://www.reseaux-telecoms.com/cso_btree/05_03_09_214614_907/CSO/Newscso_view**
- **Verdict civil rendu le 12 avril**

Dernières vulnérabilités
Autres avis (2/6)

- **Pas de scan antivirus des archives corrompues (CRC invalide)**
  - La plupart des outils de décompression répare l'archive automatiquement
- **Faille dans la décompression LHA par McAfee**
  - Tous les produits utilisant un moteur < 4400 sont exploitables
- **Vulnérabilité "Java Web Start"**
  - Affecte : Java < 1.4.2_07 et < 1.5.0_02
  - Exploit : via un fichier JNLP contenant un tag "property" malformé
- **Vulnérabilités multiples dans ASP.NET**
  - http://it-project.ru/andir/docs/aspxvuln/aspxvuln.en.xml
  - Problème de conversion des caractères Unicode 0xff00-0xffff
  - Ces caractères sont convertis en ASCII et permettent des attaques XSS

Dernières vulnérabilités
Autres avis (3/6)

- **Vulnérabilité dans le moteur MS JET 4.0**
  - **Affecte : MS JET 4.0 (msjet40.dll)**
  - **Exploit : l'ouverture d'un fichier MDB malformé par le moteur JET peut provoquer l'exécution de code**
    - **http://www.hexview.com/docs/20050331-1.txt**
  - **Pas de solution pour l'instant**

- **Traversée de répertoire via les "shell folders"**
  - **Affecte : Windows 2003**
  - **Exploit : Settings\Temp\exploit.html">Exploit**
  - **Correctif : Windows 2003 SP1**

Dernières vulnérabilités
Autres avis (4/6)

- Encore un problème de spoofing sur la barre d'état
  - Affecte : IE, Firefox (autres non testés)
  - Exploit : Utilisation d'un formulaire dans un lien
    - http://habaneronetworks.com/viewArticle.php?ID=140
- Les auteurs de Bagle, Zafi et Netsky collaborerait activement entre eux
  - http://www.kaspersky.com/news?id=160377972
- Symantec obtient un brevet sur une technologie d'analyse antivirus
  - http://www.virusbtn.com/news/virus_news/2005/03_04.xml
- Notez votre poste de travail avec PreView
  - http://www.pivx.com/preview/

Dernières vulnérabilités
Autres avis (5/6)

- Un "Vulnerability Pack" pour Immunity CANVAS
  - Une extension tierce partie contenant des 0day …
  - Exemples concernant Windows
    - Ipswitch IMail buffer overflow
    - MaxDB WebAgent stack overflow
    - Pragma Fortress buffer overflow
    - Kerio MailServer remote DoS
    - LSASS.EXE remote DoS
  - http://www.gleg.net/download/VULNDISCO.pdf

- Note : les clubs de vulnérabilités recensés
  - http://www.argeniss.com/services.html
  - http://www.idefense.com/application/poi/display?type=vulnerabilities
  - http://www.gleg.net/products.shtml
  - http://www.immunitysec.com/services-sharing.shtml

Dernières vulnérabilités
Autres avis (6/6)

- **Windows XP et Windows 2003 vulnérables à la "Land Attack"**
  - **"Land Attack" : IP source = IP destination**
  - **Chaque paquet provoque un arrêt du système de quelques secondes**
  - **On croyait cette attaque oubliée …**
- **L'attaque en "DNS poisoning" sur les produits Symantec patchée**
  - **Utilisée par des "pharmers" début mars**
  - **Il s'agissait donc d'un 0-day**
  - **http://securityresponse.symantec.com/avcenter/security/Content/2005.03.15.html**
- **Retour sur les attaques en "pharming"**
  - **http://isc.sans.org/presentations/dnspoisoning.php**

Questions / réponses

- **Questions / réponses**
- **Date de la prochaine réunion**
  - **Pas de réunion en mai pour cause de JSSI (le 10 mai)**
  - **Lundi 13 juin 2005**
- **N'hésitez pas à proposer des sujets et des salles**