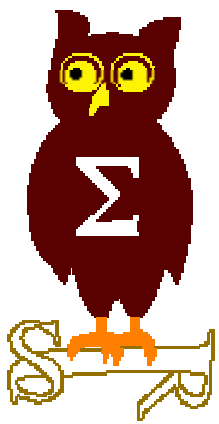
OSSIR
Groupe Sécurité Windows

Réunion du 13 mars 2006



Revue des dernières vulnérabilités Microsoft

Nicolas RUFF

EADS-CCR

nicolas.ruff@eads.net

Dernières vulnérabilités
Avis Microsoft (1/5)

- (Avis de sécurité Microsoft depuis le 13 février 2006)

- Février 2006
  - MS06-004 / Q913333 Corruption de mémoire via un fichier WMF
    - Affecte : IE toutes versions antérieures à IE6 SP1
    - Exploit :
      - Exécution de code
      - Exploitable sur Windows 2000 et XP pre-SP2

  - MS06-005 "Buffer overflow" dans le traitement des images BMP par Windows Media
    - Affecte : Windows Media toutes versions
    - Exploit : exécution de code à l'ouverture d'un .BMP/.WMP malformé
    - Crédit : Marc Maiffret

Dernières vulnérabilités
Avis Microsoft (2/5)

- MS06-006 "Buffer overflow" dans le plugin Windows Media Player
  - Affecte : Windows Media Player toutes versions
  - Exploit : exploitable via un tag "EMBED SRC=" dans un navigateur autre que IE
  - Crédit : John Cobb

- MS06-007 DoS via un paquet IGMP malformé
  - Affecte : Windows XP/2003 toutes versions
  - Exploit :déni de service distant
  - Crédit : Douglas Nascimento

- MS06-008 "Buffer overflow" dans le service WebClient
  - Affecte : Windows XP/2003 toutes versions
  - Exploit : exécution de code à distance (via un canal RPC - nécessite d'être authentifié)
  - Crédit : Kostya Kortchinsky

Dernières vulnérabilités
Avis Microsoft (3/5)

- MS06-009 Fonctions IME accessibles dans le contexte SYSTEM
  - Affecte : Windows XP/2003 Coréen, Office 2003 Coréen
  - Exploit :
    - Exécution de code dans le contexte SYSTEM
    - Accessible via la fenêtre d'authentification Terminal Server
  - Crédit : Ryan Lee

- MS06-010 Fuite d'informations dans PowerPoint
  - Affecte : Office 2000
  - Exploit : Localisation du dossier "Temporary Internet Files"
  - Crédit : Yorick Koster, Andreas Sandblad

Dernières vulnérabilités
Avis Microsoft (4/5)

- **Mars 2006**
  - 1 bulletin critique Office
  - 1 bulletin important Windows
  - 1 mise à jour non sécurité pour MU et WSUS

- **Advisories**
  - Q906267 MSDDS.DLL provoque un DoS dans IE
    - Reconnaît que le problème a été fixé dans MS05-052
  - Q914457 Attaque "Winval"
    - Microsoft indique que Windows XP SP2 et Windows 2003 SP1 ne sont pas vulnérables
  - Q912945 Mise à jour pour IE

Dernières vulnérabilités
Avis Microsoft (5/5)

- **Révisions**
  - **Q914457 Permissions Windows trop laxistes**
  - **Q913333 -> MS06-004**
  - **MS06-009**
    - **Version 1.1**
  - **MS06-007 DoS via un paquet IGMP malformé**
    - **Version 1.1 Déploiement automatique via WUS, SUS, …**
  - **MS06-005**
    - **Version 1.2 Problème avec WMP 10**
  - **MS05-054**
    - **Version 1.2 Référence CAN-2005-1790**
  - **MS05-013**
    - **Version 1.2 Référence Q906216 (problème avec dhtmled.ocx)**

Dernières vulnérabilités
Infos Microsoft (1/1)

- **Monad Beta 3.1**
  - http://go.microsoft.com/?linkid=4615390
- **Microsoft Office Live**
  - http://officelive.microsoft.com/
  - La réponse à SalesForce.com ?
- **Windows Antispyware Beta1 identifie les produits Symantec comme des spywares**
  - http://www.techweb.com/wire/180200671
- **Windows Defender Beta2**
  - La suite de Microsoft Antispyware Beta1
  - http://www.microsoft.com/downloads/details.aspx?familyid=435BFCE7-DA2B-4A6A-AFA4-F7F14E605A0D&displaylang=en
- **Microsoft se prononce contre la prime iDefense**
  - +$10,000 pour une faille "critique"
  - http://www.eweek.com/print_article2/0,1217,a=171828,00.asp

Dernières vulnérabilités
Autres avis (1/6) - failles

- La faille WMF a été vendue par un Russe à une société de spyware
  - Prix : $4,000
  - Date : autour du 1er décembre
  - http://www.computerworld.com/printthis/2006/0,4814,108355,00.html

- Vulnérabilité "Drag and Drop" dans IE
  - Affecte : IE toutes versions
  - Exploit :
    - Permet le contournement des restrictions de sécurité
    - L'utilisateur doit faire un "drag and drop" dans IE (!)
  - Crédit : Matthew Murphy

  - Ne sera pas corrigée avant le prochain SP
    - http://www.computerworld.com/printthis/2006/0,4814,108654,00.html

Dernières vulnérabilités
Autres avis (2/6) - failles

- **Vulnérabilités IE**
  - DoS via URLMON.DLL
    - Affecte : IE 7 Beta 2 (autres non testés)
    - http://www.securityfocus.com/bid/16463
  - DoS via JScript embarqué dans un ActionScript (Flash)
    - http://www.securityfocus.com/bid/16441
  - "Buffer overflow" dans VBScript/JScript
    - Exploit : http://www.anspi.pl/~fex/recurrboom.html
  - DoS via une Applet Java (machine Sun)
    - http://www.securityfocus.com/bid/16978
    - Exploit : http://www.anspi.pl/~fex/rx6502.html
  - "Buffer overflow" dans IsComponentInstalled()
    - Corrigé silencieusement dans les versions récentes d'IE
    - http://www.securityfocus.com/bid/16870
    - Exploit : ie_iscomponentinstalled.pm (Metasploit)

Dernières vulnérabilités
Autres avis (3/6) – virus et spywares

- Un "virus" MacOS X
  - Fichier .tgz se propageant par messagerie et iChat
  - Prétend être une preview de "Mac OS X Leopard" ☺
  - Plusieurs versions en circulation

- Des virus BlueTooth pour Nokia Series 60
  - SymbOS.Sendtool.A
  - SymbOS.Pbstealer.D
  - SymbOS.Bootton.E

- Le virus "Crossfire" objet de litige entre les éditeurs antivirus et la MARA (Mobile Antivirus Research Association)
  - http://www.securityfocus.com/news/11379
  - Virus trans-platformes (PC -> Windows Mobile) dont seule la MARA détient la souche

- 8 ans de prison pour avoir volé 1 milliard d'adresses email
  - http://news.com.com/2102-7348_3-6042290.html?tag=st.util.print

Dernières vulnérabilités
Autres avis (4/6) – virus et spywares

- Les utilisateurs d'IE ont 20x plus de chances d'attraper un spyware que les utilisateurs de FireFox
  - http://www.informationweek.com/security/showArticle.jhtml%3B?articleID=179102695
- Un spyware "dormant" détourne 1 million d'euros en France
  - Se réveille sur la connexion à une banque en ligne
  - Opération organisée depuis l'Ukraine
  - http://www.guardian.co.uk/print/0,,5393279-110633,00.html
  - Information fiable ? Semble peu crédible vu les fraudes antérieures …
- Le nombre de sites de phishing a doublé en décembre 2005 suite à la publication d'un toolkit
  - http://www.zdnet.com.au/news/security/print.htm?TYPE=story&AT=39240328-2000061744t-10000005c
- AOL poursuit en justice les groupes de phishing
  - http://software.silicon.com/security/0,39024655,39156840,00.htm

Dernières vulnérabilités
Autres avis (5/6)

- Symantec abandonne L0phtCrack
  - http://www.securitydump.com/content160.html
  - Nombreuses alternatives (ex. LCP)
- IBM Allemagne ira sur Linux plutôt que Vista
  - http://www.pcinpact.com/actu/news/27145-IBM-ne-migrera-pas-vers-Windows-Vista.htm?vc=1
- ZoneAlarm 6.0, un spyware ?
  - http://www.infoworld.com/article/06/01/13/73792_03OPcringley_1.html
- Le Royaume-Uni va-t-il demander à Microsoft de mettre une backdoor dans Vista ?
  - Fonctions de sécurité basées sur le TPM réputées "inviolables"
    - Ex. chiffrement BitLocker
  - http://news.bbc.co.uk/1/hi/uk_politics/4713018.stm

Dernières vulnérabilités
Autres avis (6/6)

- **Yahoo et AOL relance l'idée de l'email payant**
  - **http://news.bbc.co.uk/2/hi/technology/4684942.stm**
  - **Les associations caritatives se prononcent contre**
    - **http://news.bbc.co.uk/1/hi/technology/4778136.stm**

Questions / réponses

- Questions / réponses
- Date de la prochaine réunion
  - 10 avril 2006
- N'hésitez pas à proposer des sujets et des salles