EdelWeb

OSSIR
Groupe Sécurité Windows

Réunion du 8 mars 2004

Revue des dernières vulnérabilités Windows

Nicolas RUFF

nicolas.ruff@edelweb.fr

Dernières vulnérabilités
Avis Microsoft (1/2)

EdelWeb

- **Avis de sécurité Microsoft depuis le 09/02/2004**
  - **MS04-005 Vulnérabilité Virtual PC**
    - **Affecte : Virtual PC pour Mac 6.0 - 6.1**
    - **Exploit : élévation de privilèges locale**
    - **Source : @stake**
      - **http://www.atstake.com/research/advisories/2004/a021004-1.txt**
  - **MS04-006 Vulnérabilité dans le service WINS**
    - **Affecte : Windows NT4 - 2003**
    - **Exploit : déni de service sur Windows 2003 uniquement, à cause du mécanisme de "stack protection" !**
    - **Source : Qualys**

Dernières vulnérabilités
Avis Microsoft (2/2)

EdelWeb

- MS04-007 Vulnérabilité dans le décodeur ASN1
  - Affecte : Windows NT4 – 2003
    - Au moins vulnérables :
      - Kerberos (UDP/88)
      - NTLMv2 (TCP/135, TCP/139, TCP/445)
      - HTTPS sur IIS (TCP/443)
  - Affecte également : Windows 98
    - Mise à jour tardive de Microsoft
  - Affecte les dispositifs de VoIP basés sur du code partagé ?
    - Ex. Cisco – cf. vulnérabilité H323
  - Exploit : exécution de code à distance
  - Source : eEye
    - http://www.eeye.com/html/Research/Advisories/AD20040210.html
    - http://www.eeye.com/html/Research/Advisories/AD20040210-2.html
    - Reporté à Microsoft depuis 6 mois

- Les vulnérabilités en attente …
  - http://www.eeye.com/html/Research/Upcoming/index.html

Dernières vulnérabilités
Infos Microsoft (1/4)

EdelWeb

- "We have never had vulnerabilities exploited before the patch was known"
  - http://news.bbc.co.uk/1/hi/technology/3485972.stm
- "Windows 95 was written without a single security feature, he said, as it was designed to be totally open to let users connect to other systems. Furthermore, the security kernel of the Windows NT server software was written before the Internet, and the Windows Server 2003 software was written before buffer overflows became a frequent target of recent attacks..."
  - http://www.infoworld.com/article/04/02/24/HNunderattack_1.html
- "Grâce au patch MS04-004, IE est le navigateur le plus sécurisé existant actuellement"
  - http://news.zdnet.co.uk/0,39020330,39146084,00.htm

- Vulnérabilité IE critique non patchée
  - Affecte : IE 5.0 – 6.0
  - Exploit :
    - ms-its:mhtml:file://C:\ss.MHT!http://www.test.com//chm.chm::/vir/virus.htm
  - Workaround :
    - Modifier l'entrée HKCR\Protocols\Handler\ms-its
  - Crédit : Thor Larholm
  - Exploitée par le ver Ibiza

Dernières vulnérabilités
Infos Microsoft (2/4)

EdelWeb

- Plan de retrait Windows 2000 Server
  - 1er avril 2004 : fin des licences en volume
  - 1er novembre 2004 : fin des licences OEM
  - 31 mars 2005 : fin du support technique
  - 1er novembre 2005 : fin de la vente aux intégrateurs
  - 1er avril 2006 : fin complète de distribution du produit
  - 31 mars 2007 : fin du support technique étendu

- Active Directory Migration Tool (ADMT) v2
  - http://www.microsoft.com/windows2000/downloads/tools/admt/default.asp
  - http://support.microsoft.com/default.aspx?scid=kb;FR;326480

- Code source de Windows disponible sur les réseaux P2P
  - http://www.microsoft.com/presspass/press/2004/Feb04/02-12windowssource.asp
  - Environ 660 Mo de fichiers texte
    - Entre 1/1000 et 1/3 du code selon les estimations
  - Source de la fuite : Mainsoft ?
    - http://www.eweek.com/article2/0,4149,1526830,00.asp
    - Version : Windows 2000 SP1, 25 juillet 2000

Dernières vulnérabilités
Infos Microsoft (3/4)

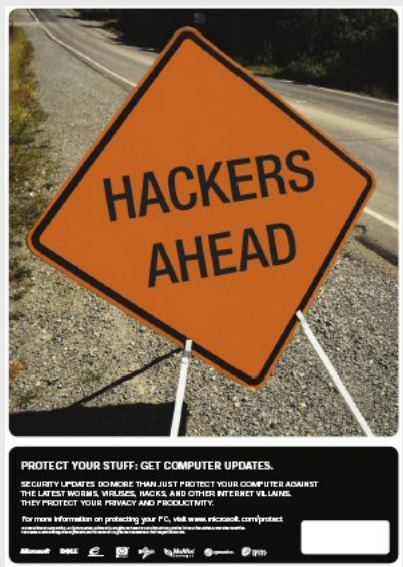
EdelWeb

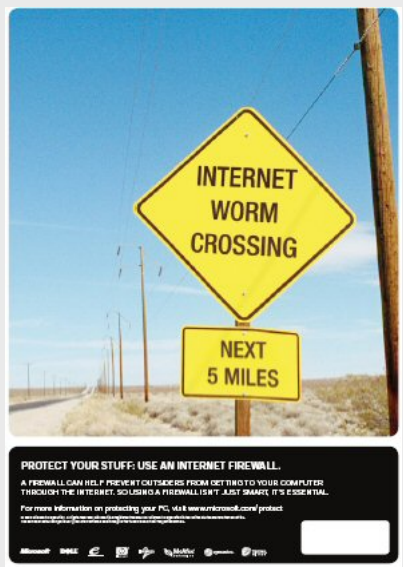
- Site en français dédié aux professionnels de la sécurité
  - http://www.microsoft.com/france/securite/it/default.mspx
- Lutte contre le spam avec "Caller ID"
  - Identification de l'émetteur par interrogation DNS
  - http://www.microsoft.com/mscorp/twc/privacy/spam_callerid.mspx
- Autres idées :
  - Sender Policy Framework
    - DNS également
    - http://spf.pobox.com/
  - DomainKeys (Yahoo)
    - Signature de tous les messages par PGP sur le serveur

Dernières vulnérabilités
Infos Microsoft (4/4)

EdelWeb

- **Services for Unix 3.5**
  - **Gratuit mais enregistrement nécessaire (Passport)**
  - **http://www.microsoft.com/windows/sfu/downloads/default.asp**
- **Des posters à télécharger**
  - **http://www.microsoft.com/education/?ID=SecurityPosters**





Dernières vulnérabilités
Autres avis (1/4)

EdelWeb

- Ver Vesser / Deadhat
  - Infecte les machines via la "backdoor" MyDoom
  - Désinstalle MyDoom et installe sa propre backdoor !
- Ver DoomJuice
  - Infecte les machines via la "backdoor" MyDoom
  - DoS contre www.microsoft.com
- Ver Netsky
- Ver Bagle.{A - I}
  - Utilise un fichier ZIP avec mot de passe
  - Techniques de Social Engineering élaborées
- Etc. etc.

- Les utilisateurs du FAI "Sonera" reçoivent des "returned mails" provenant de "echelon@sonera.inet.fi"
- Le "blackout aux Etats-Unis lié à une erreur de programmation dans la gestion des erreurs ?
  - http://www.cnn.com/2004/US/Northeast/02/13/blackout.ap/index.html
- Créer un CD Windows bootable avec BartPE
  - http://www.nu2.nu/pebuilder/

Dernières vulnérabilités
Autres avis (2/4)

EdelWeb

- "Buffer overflow" dans le gestionnaire d'appels "hcp://"
  - Affecte : Windows XP SP1
  - Exploit : permet l'exécution de code dans le contexte de l'utilisateur courant
  - http://www.securityfocus.com/bid/9621/

- "Buffer overflow" dans le décodage des fichiers EMF
  - EMF = Encapsulated MetaFile = format standard Windows d'image vectorielle
  - Affecte : tout logiciel utilisant le moteur de rendu Microsoft (IE, Outlook, Word, etc.)
  - Exploit : non disponible

Dernières vulnérabilités
Autres avis (3/4)

EdelWeb

- "Buffer overflow" dans le système d'annotation d'Acrobat Reader
  - Affecte : Acrobat Reader 5.1
  - Exploit : un objet de type MIME "application/vnd.adobe.xfdf" est automatiquement rendu dans IE / Outlook

- "Buffer overflow" dans WinZip
  - Affecte : WinZip jusqu'à 8.0 (9.0 non vulnérable)
  - Exploit : "buffer overflow" exploitable avec les extensions
    - .mim, .uue, .uu, .b64, .bhx, .hqx, .xxe

Dernières vulnérabilités
Autres avis (4/4)

EdelWeb

- **Vulnérabilités IE**
  - **Énumération de fichiers via LoadPicture()**
    - **Exploit : appel de la fonction LoadPicture() en VBScript**
    - **http://www.securityfocus.com/bid/9611**
  - **"Cross-zone scripting" via un IFRAME**
    - **Exploit : non disponible**
    - **http://www.securityfocus.com/bid/9628**
  - **Déni de service IE/Outlook**
    - **Exploit : utilisation de deux caractères nuls consécutifs**
    - **http://www.securityfocus.com/bid/9629/**
  - **Lecture de données dans le presse-papiers**
    - **Exploit : execCommand("Paste")**
    - **http://www.securityfocus.com/bid/9643**
  - **Exécution de code en zone "poste de travail"**
    - **Exploit : external.NavigateAndFind('res://<fichier local>','','')**
    - **http://www.securityfocus.com/bid/9568**

Questions / réponses

EdelWeb

- **Questions / réponses**
- **Date de la prochaine réunion :**
  - **Lundi 5 avril 2004**
- **N'hésitez pas à proposer des sujets et des salles**