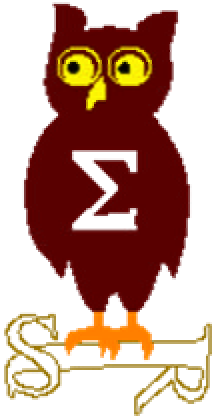
EdelWeb

OSSIR
Groupe Sécurité Windows

Réunion du 13 janvier 2003



EdelWeb

Revue des dernières vulnérabilités Windows

Nicolas RUFF

nicolas.ruff@edelweb.fr

Dernières vulnérabilités
Avis Microsoft (1/2)

- **Avis de sécurité Microsoft depuis le 09/12/2002**
  - **MS02-069 : patch cumulatif pour la JVM MS**
    - **Affecte principalement IE / Outlook**
    - **Nouvelles vulnérabilités :**
      - **Accès aux objets COM par une applet « untrusted »**
      - **Modification du « codebase » de l'applet et donc de la zone de sécurité**
      - **Accès illimité à l'API JDBC**
      - **Accès illimité à l'API de sécurité permettant de bannir des applets**
      - **Détection du nom de login via la propriété « user.dir »**
      - **Déni de service IE par instanciation incomplète d'une autre applet**
  - **MS02-070 : vulnérabilité dans la signature SMB**
    - **Affecte Windows 2000 et Windows XP**
    - **Détails :**
      - **Le mécanisme de signature SMB est une nouveauté de Windows 2000**
      - **Il n'est pas activé par défaut**
      - **Attaque en « downgrade » possible**
    - **La principale conséquence d'après MS est la modification à la volée des stratégies de groupe lors de leur chargement**
      - **Cette attaque est donc possible lorsque la signature SMB n'est pas activée !!!**
    - **Fixé silencieusement dans Windows XP SP1**

Dernières vulnérabilités
Avis Microsoft (2/2)

- **MS02-071 : vulnérabilité WM_TIMER**
  - **Affecte Windows NT4, 2000, XP**
  - **La fonction de callback appellée à l'expiration du timer peut être n'importe quelle fonction du système (!)**
  - **Permet à l'utilisateur interactif d'obtenir des droits SYSTEM**
  - **Patch très instable**
- **MS02-072 : débordement de buffer dans le shell**
  - **Affecte Windows XP**
  - **Débordement de buffer dans le traitement d'un attribut étendu**
  - **La prévisualisation d'un fichier WMA ou MP3 suffit à exécuter du code dans le contexte de l'utilisateur**

- **Bulletins mis à jour depuis le 09/12/2002**
  - **Aucun**

Dernières vulnérabilités
Infos Microsoft (1/2)

EdelWeb

- Sortie du MBSA 1.1
  - Supporte maintenant Windows Media Player, SQL Server, Exchange
  - Inclus HFNetChk 3.81
  - Compatible MSUS, SMS 2.0
  - http://www.microsoft.com/technet/security/tools/Tools/MBSAhome.asp
- Modèle de déploiement AD par MS Consulting
  - http://www.microsoft.com/france/windows/2000/server/info/20021203_modele_deploiement_ad.html
- Communication vers le grand public
  - Glossaire sécurité
    - http://www.microsoft.com/france/securite/glossaire/default.asp
    - Ne connaît pas les mots « bug », « bogue » et « vulnérabilité »
  - La sécurité de A à Z
    - http://www.microsoft.com/france/securite/grandpublic/secu_informatique_az/default.asp
    - Ne considère que 4 risques : virus, ver, cheval de Troie et macro-virus !

Dernières vulnérabilités
Infos Microsoft (2/2)

- « Simulateurs » Windows
  - http://www.laboratoire-microsoft.org/simulateurs/
- Feature Pack 1 pour ISA Server
  - http://www.microsoft.com/isaserver/featurepack1/overview/
  - Filtre anti-spam
  - URLScan 2.5
  - Authentification Web SecurID
  - Supporte OWA
  - Proxy RPC
  - Etc.

Dernières vulnérabilités
Autres avis (1/1)

- **Nouvelles checklists de sécurité (en anglais)**
  - **Windows XP : http://www.labmice.net/articles/winxpsecuritychecklist.htm**
  - **Windows 2000 : http://www.labmice.net/articles/securingwin2000.htm**
- **IEHK**
  - **Internet Explorer Hacking Kit**
  - **http://valgasu.rstack.org/**
- **SMAC**
  - **Permet de changer de manière permanente l'adresse MAC d'une carte réseau (mémorisé dans la registry)**
  - **NdisReadNetworkAddress()**
  - **http://www.klcconsulting.net/smac/**

Questions / réponses

EdelWeb

- **Questions / réponses**
- **Date de la prochaine réunion :**
  - **Lundi 10 février 2003**
  - **Nous recherchons des sujets**
    - **Sujets pressentis : OWA, fuite d'information dans Office, retour d'expérience sur la mise en œuvre de la signature partagée avec PGP**
  - **Nous recherchons des salles**
- **Rappel : JSSI le 3 avril 2003**