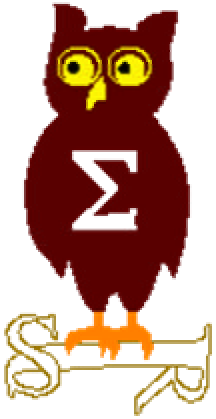
EdelWeb

OSSIR
Groupe Sécurité Windows

Réunion du 11 février 2002



EdelWeb

Revue des dernières vulnérabilités de Windows 2000

Nicolas RUFF

nicolas.ruff@edelweb.fr

Dernières vulnérabilités (1/4)

EdelWeb

- **Avis de sécurité Microsoft depuis le 17/12/2001 :**
  - **MS01-059 : exploit SYSTEM distant / déni de service sur UPNP**
    - **Windows 98, ME, XP**
    - **Vulnérabilités multiples**
      - **Déni de service UDP/1900**

      + Possibilité « Distributed DOS »
      - **Déni de service TCP/5000**
      - **Shell SYSTEM TCP/5000**
    - **Avis du FBI**
  - **MS01-060 : « buffer overflow » dans SQL Server 7 et 2000**
    - **Lié à MSVCRT.DLL**
  - **MS02-001 : exploitation des relations d'approbation explicites**
    - **Le domaine « trustant » ne vérifie pas si le domaine « trusté » fait autorité pour les SID fournis dans le jeton**

Dernières vulnérabilités (2/4)

- MS02-002 : déni de service sur Office pour MacOS X
  - Lié au service réseau « anti-piratage » (!)
- MS02-003 : l'agent d'administration Exchange 2000 diminue le niveau de sécurité du système
  - Permission « Everyone » sur la clé WinReg
  - Autorise l'accès distant à la base de registre
- MS02-004 : exploit Telnet sur Windows 2000 et Interix 2.2
  - Exploitable à distance
  - Droits SYSTEM

- Programme « Gold Certified Partner Program for Security Solutions »
- Sortie du SRP1
  - Nécessite un reboot immédiat !
- « Security Toolkit » disponible dans PCExpert en France

Dernières vulnérabilités (3/4)

- **Autres avis : Windows**
  - **DoS sur les stratégies de groupe par verrouillage de fichier**
    - **Le système permet d'ouvrir un fichier en mode exclusif même si les permissions d'accès n'autorisent aucun accès**
  - **Vulnérabilités XP**
    - **« Fast user switching » et « account lockout » incompatibles**
    - **« Password reset disk » et « minimum password age » incompatibles**
    - **« Remote Desktop » envoie le nom de login en clair sur le réseau**
    - **Pour info : le « fingerprint » de la licence est stocké dans le fichier wpa.dbl**
  - **Vulnérabilités .NET beta3**
    - **http://dotnet.microsoft.com/<script>alert(document.cookie)</script>.aspx**

Dernières vulnérabilités (4/4)

EdelWeb

- « Bunratty » attack
  - Création d'un dossier « caché » où sont envoyées des commandes et des mises à jour pour un cheval de Troie implanté sur la cible
  - http://www.itsecurity.com/papers/andyclarke.htm
  - Bunratty est un château irlandais
- Microsoft Site Server 3.0 [RFP]
  - Nombreuses vulnérabilités, ex. mots de passe « en dur »
- Vulnérabilités Internet Explorer
  - GetObject() permet de lire des fichiers du disque dur
  - « Extended HTML Form Attack »
    - « Cross-site scripting »
    - POST sur un port qui retourne les données transmises
    - http://eyeonsecurity.net/advisories/showMyCookie.html

Questions / réponses

EdelWeb

- Questions / réponses
- Date de la prochaine réunion : 11 mars 2002