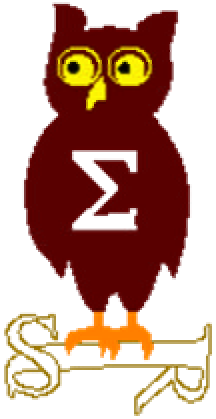
EdelWeb

OSSIR
Groupe Sécurité Windows

Réunion du 11 mars 2002



Revue des dernières vulnérabilités de Windows 2000

Nicolas RUFF

nicolas.ruff@edelweb.fr

Dernières vulnérabilités (1/3)

- **Avis de sécurité Microsoft depuis le 11/02/2002 :**
  - **MS02-005 : patch cumulatif pour IE (6 vulnérabilités)**
    - **« Buffer overrun » dans un tag HTML**
    - **Lecture de fichiers par GetObject()**
    - **Affichage erroné dans la boîte de dialogue « téléchargement »**
    - **« Content-type » MIME ? extension du fichier permet l'exécution de pièces jointes sans confirmation**
    - **Exécution de scripts même si ceux-ci ont été désactivés**
    - **Lecture de fichiers par une variante de « frame domain verification »**
  - **MS02-006 : exploit SYSTEM sur SNMP**
    - **Découvert à partir d'un outil de test d'implémentation automatisé de l'université d'OULU (cf. outil LDAP)**
    - **Nombreux systèmes affectés (cf. avis du CERT)**
  - **MS02-007 : exploit distant sur SQL Server 7.0 et 2000**
    - **SQL ne s'exécute pas forcément dans le contexte SYSTEM**

Dernières vulnérabilités (2/3)

- MS02-008 : erreur de conception dans le contrôle XMLHTTP
  - Permet à une page Web hostile de lire n'importe quel fichier du disque dur
- MS02-009 : « cross-scripting » entre pages Web avec IE
  - Idem
- MS02-010 : exploit SYSTEM distant dans Commerce Server 2000
  - Le filtre ISAPI AuthFilter contient un débordement de buffer
- MS02-011 : erreur dans l'authentification SMTP (Windows 2000, Exchange 5.5)
  - Autorise le « relaying » anonyme
- MS02-012 : déni de service SMTP (Exchange 2000, Windows 2000, Windows XP)
- MS02-013 : vulnérabilité JVM (IE 4.x, IE 5.x)
  - Permet à une applet de modifier les paramètres du proxy

Dernières vulnérabilités (3/3)

- **Autres avis**
  - **Cigital prétend que le compilateur .NET introduit des vulnérabilités dans les programmes compilés**

Questions / réponses

EdelWeb

- **Questions / réponses**

- **Date de la prochaine réunion :**
  - **JSSI 9 avril 2002**
  - **13 mai 2002**