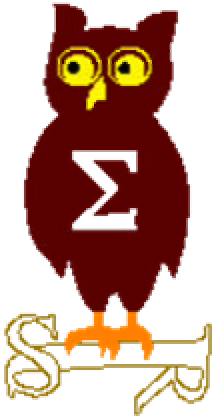
EdelWeb

OSSIR
Groupe Sécurité Windows

Réunion du 10 juin 2002



EdelWeb

Revue des dernières vulnérabilités de Windows 2000

Nicolas RUFF

nicolas.ruff@edelweb.fr

Dernières vulnérabilités (1/2)

EdelWeb

- **Avis de sécurité Microsoft depuis le 13/05/2002**
  - **MS02-023 : Patch cumulatif pour IE 5.01, 5.5 et 6.0**
    - **Corrige 6 vulnérabilités**
      - **Cross-site scripting**
      - **Lecture de fichiers**
      - **Lecture de cookies**
      - **Spoofing de zone**
      - **2 variantes de MS01-058 (types MIME erronés)**
  - **MS02-024 : Patch contre « DebPloit »**
    - **Exploitable pendant 6 ans …**
  - **MS02-025 : Déni de service sur Exchange 2000**
    - **Par entêtes SMTP malformés**
  - **MS02-026 : « Buffer overflow » dans le service ASP.NET Worker**
    - **Déni de service (redémarrage du service)**
    - **Exploitable ?**

Dernières vulnérabilités (2/2)

- **Autres**
  - **Ver Spida**
    - **S'attaque aux comptes « SA » sans mot de passe sur SQL Server**
  - **Advisory Guninski #55**
    - **Les « stylesheets » XML sous Excel permettent d'exécuter du code**
  - **Au cours du procès « antitrust », Monsieur Allchin (vice-président Microsoft) a déclaré que le code Microsoft était tellement bogué qu'il était impossible de le publier**
    - **Les API Message Queue et WFP ont été mentionnées**
  - **« Buffer overflow » dans Macromedia JRun 3.1 pour IIS 4 et 5**
  - **Vulnérabilité « gopher:// » dans Internet Explorer**
    - **http://www.solutions.fi/index.cgi/news_2002_06_04?lang=eng**

Questions / réponses

EdelWeb

- **Questions / réponses**

- **Date de la prochaine réunion :**
  - **Lundi 8 juillet 2002**