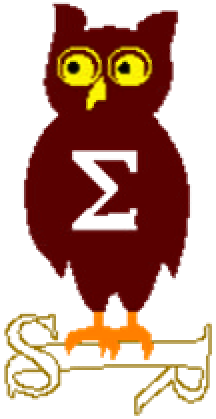
EdelWeb

OSSIR
Groupe Sécurité Windows

Réunion du 8 juillet 2002



Revue des dernières vulnérabilités de Windows 2000

Nicolas RUFF

nicolas.ruff@edelweb.fr

Dernières vulnérabilités (1/3)

- **Avis de sécurité Microsoft depuis le 10/06/2002**
  - **MS02-022 v2 : variantes de la vulnérabilité MSN**
    - **Affecte MSN Chat ActiveX**
    - **Permet l'exécution de code dans le contexte utilisateur par débordement de buffer**
  - **MS02-027 v1 et v2 : vulnérabilité « gopher:// »**
    - **Affecte IE, Proxy Server et ISA Server**
    - **Permet l'exécution de code dans le contexte utilisateur par débordement de buffer**
  - **MS02-028 v1 et v2 : vulnérabilité dans le filtre ISAPI « .htr »**
    - **Affecte IIS4 et IIS5**
    - **Permet l'exécution de code dans le contexte IWAM_computer par débordement de buffer**
  - **MS02-029 v1 et v2 : vulnérabilité dans l'annuaire du service RAS**
    - **Affecte Windows NT4 / 2000 / XP**
    - **Permet l'exécution de code dans le contexte SYSTEM par débordement de buffer**
    - **Requière un compte utilisateur sur le système**

Dernières vulnérabilités (2/3)

- MS02-030 : 2 vulnérabilités SQLXML 3 + IIS 5 + SQL Server 2000
  - Cross-site scripting
  - « Buffer overflow » dans le filtre ISAPI
- MS02-031 : exécution de macros dans Word, Excel et Office XP
- MS02-032 : patch cumulatif pour Windows Media Player 6.4, 7.1 et XP
  - 3 nouvelles vulnérabilités
  - Exécution de code et de scripts dans le contexte utilisateur, élévation de privilèges vers SYSTEM
- MS02-033 : 4 vulnérabilités dans Commerce Server 2000 et 2002
  - Permet l'exécution de code dans le contexte SYSTEM par débordement de buffer

Dernières vulnérabilités (3/3)

- **Autres**
  - **Vulnérabilité SQL Server 2000**
    - **Vulnérabilité OpenDataSource + MS Jet Engine**
    - **« Buffer overflow » exploitable**
    - **Patch Q282010**
  - **Visual Studio .NET coréen est infecté avec Nimda**
  - **Répertoire WEB-INF accessible**
    - **Serveurs Windows exécutant J2EE Servlets**
  - **Vulnérabilités JRun 4.0 sur Windows 2000**
    - **« Source disclosure »**
    - **Accès à la console admin (en ajoutant // à la fin de l'URL …)**

Questions / réponses

EdelWeb

- **Questions / réponses**

- **Date de la prochaine réunion :**
  - **Lundi 9 septembre 2002**