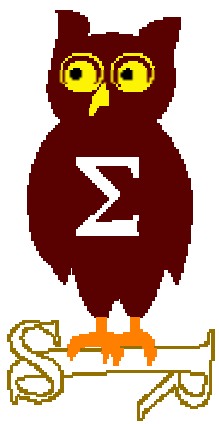
OSSIR
Groupe Sécurité Windows

Réunion du 10 octobre 2005



Revue des dernières vulnérabilités Microsoft

Nicolas RUFF

EADS-CCR

nicolas.ruff@eads.net

Dernières vulnérabilités
Avis Microsoft (1/1)

- (Avis de sécurité Microsoft depuis le 12 septembre 2005)

- Septembre 2005
  - Pas de bulletins de sécurité
  - Bulletins "non sécurité"
    - Microsoft Update (MU)
    - Windows Update (WU)
    - Windows Server Update Services (WSUS)
    - Software Update Services (SUS)

- Octobre 2005
  - 8 bulletins Windows allant jusqu'à "critique"
  - 1 bulletin Windows + Exchange "important"

Dernières vulnérabilités
Infos Microsoft (1/2)

- **Sortie du SRP1 v2**
  - **Affecte : Windows 2000 SP4**
  - **Sortie le 13 septembre 2005**
  - **Cf. Q891861**
- **Sortie de SQL Server 2005 en novembre**
  - **A cette occasion, MSDE est remplacé par SQL Server 2005 Express Edition**
- **Preview de la prochaine version d'Office**
  - **http://pdc.xbetas.com/?page=o12preview1**
- **"GAGNE des paramètres de registre pour Windows 2000"**
  - **http://support.microsoft.com/default.aspx?scid=kb;FR;q251067**

Dernières vulnérabilités
Infos Microsoft (2/2)

- **Quelques nouveautés de Windows Vista**
  - **Un système de fichiers supportant le SetUID !**
    - **Utilisé par IE 7**
  - **Un contrôle des communications inter-fenêtres**
    - **Pour lutter contre les Shatter Attacks**
  - **Une gestion des sockets en mode noyau**
  - **IPv6 actif par défaut**

Dernières vulnérabilités
Autres avis (1/2)

- Une base de BHO contenant 7000 objets …
  - http://castlecops.com/CLSID.html
- Des avis de sécurité sur des logiciels Windows Mobile
  - Affecte : vxTftpSrv, vxWeb, TTXN File Transfer Anywhere
  - Exploit : exécution de code
  - Crédit : Seth Fogie (Airscanner)
- Abus du mécanisme de détection de type
  - Affecte : IE
  - Exploit : <GIF89a …
- Injection de commandes via le contrôle ActiveX XMLHTTP
  - Affecte : IE 6
  - Exploit : appel de la méthode open() avec des séparateurs non standard
    - Cf. http://secunia.com/advisories/16911/
  - Remarque : la méthode XmlHttpRequest, au cœur du système AJAX (Asynchronous Javascript And XML), est dispo sur IE et Mozilla.
  - On a pas fini d'en entendre parler …

Dernières vulnérabilités
Autres avis (2/2)

- **Preview "non officielle" du SP3 pour Windows XP**
  - http://www.thehotfix.net/sp3.html
  - Note : IE 7 ne sera pas intégré au SP3
- **Bug dans "Wireless Zero Configuration Service"**
  - Affecte : Windows XP
  - Exploit : permet à un attaquant local non privilégié de récupérer les clés WEP et PMK par un appel à WZCQueryInterface()
  - Correctif : Windows Longhorn ☺
  - Crédit : Laszlo Toth
- **La note CD sur Skype …**
  - http://www.spyworld-actu.com/article.php3?id_article=834

Questions / réponses

- **Questions / réponses**
- **Date de la prochaine réunion**
  - **Lundi 7 novembre 2005**
- **N'hésitez pas à proposer des sujets et des salles**