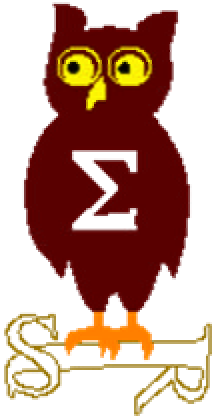
EdelWeb

OSSIR
Groupe Sécurité Windows

Réunion du 10 mars 2003



EdelWeb

Revue des dernières vulnérabilités Windows

Nicolas RUFF

nicolas.ruff@edelweb.fr

Dernières vulnérabilités
Avis Microsoft (1/2)

EdelWeb

- **Avis de sécurité Microsoft depuis le 13/01/2003**
  - **MS03-001 : débordement de buffer dans le service « MS Locator »**
    - **Affecte MS Locator, dont le rôle est des transcrire des noms logiques en adresses IP**
    - **Démarré par défaut sur les PDC Windows NT4 et 2000**
    - **Peut être démarré sur toute machine Windows NT4 / 2000 / XP**
  - **MS03-002 : patch cumulatif pour MCMS 2001**
    - **Affecte Microsoft Content Management Server (MCMS) 2001**
    - **Il existe un faille de type Cross Site Scripting**
  - **MS03-003 : vulnérablité d'implémentation cryptographique dans Outlook 2002**
    - **Affecte Outlook 2002**
    - **N'affecte que les certificats Exchange Server Security V1 (et non S/MIME)**
    - **Le chiffrement du message échoue silencieusement et le message passe en clair**

Dernières vulnérabilités
Avis Microsoft (2/2)

- MS03-004 : patch cumulatif pour IE
  - Affecte IE 5.01, IE 5.5, IE 6.0
  - 2 nouvelles vulnérabilités « cross-domain »
  - Conséquences : lecture de fichiers locaux, exécution de programmes locaux
- MS03-005 : débordement de buffer dans le redirecteur
  - Affecte Windows XP
  - Permet une élévation de privilèges vers SYSTEM
- MS03-006
  - Affecte Windows ME
  - Débordement de buffer dans le support du protocole hcp://

- Bulletins mis à jour depuis le 13/01/2003
  - MS02-071 v2 : vulnérabilité WM_TIMER
    - Patch Windows NT4 instable
  - MS03-004 v2 : patch cumulatif pour IE
    - Dysfonctionnement dans l'authentification

Dernières vulnérabilités
Infos Microsoft (1/4)

- Ver « SQL/Sapphire » ou « SQL/Slammer »
  - Exploite MS02-061 (connu depuis 6 mois)
  - Plus petit ver connu (376 octets)
  - Nombreuses spéculations sur son origine
    - David Litchfield, groupe terroriste, Kevin ☺ …
  - Portée mondiale
    - Touche Microsoft
      - http://news.zdnet.fr/story/0,,t118-s2129474,00.html?nl=zdtech
      - http://www.theregister.co.uk/content/56/29073.html
    - Touche les distributeurs Bank of America
  - « Zi Hackademy » cités en experts techniques sur France 2
  - Liste des applications installant MSDE
    - http://www.sqlsecurity.com/DesktopDefault.aspx?tabindex=10&tabid=13
  - Outils de détection de MSDE
    - http://www.microsoft.com/sql/downloads/securitytools.asp
  - Correctifs
    - Hotfix ou SP3
    - Impacts du SP3 non négligeables

Dernières vulnérabilités
Infos Microsoft (2/4)

EdelWeb

- SP1a pour Windows XP
  - http://www.microsoft.com/france/windows/xp/pro/telecharge/info/20030213_sp1a.html
- SP1 pour MSUS
- SP3 pour Exchange 2000
  - *Administrabilité*
    - meilleur reporting des erreurs
    - administration multi-serveurs facilitée
    - nouvelle API de surveillance facilitant les diagnostics
  - *Performance*
    - support du contrôleur Fibre Channel SANBlade de QLogic
  - *Sécurité*
    - mise à jour des *SQL Server Books Online*, qui fournissent des conseils de sécurisation
    - correctifs de sécurité
    - possibilité d'exécuter le SQL Server Agent sans être administrateur
- SP2a pour SharePoint Portal 2001

Dernières vulnérabilités Infos Microsoft (3/4)

EdelWeb

- "Controlling Communication with the Internet" (178 p.)
  - Série "Using Windows XP Pro with SP1 in a Managed Environnement"
  - Dispo sur http://technet.microsoft.at/includes/file.asp?ID=4668
- « Palladium » devient « Next Generation Secure Computing Base »
- Ouvrage « Sécurité sous Microsoft Windows 2000 et Microsoft Windows XP »
  - En Français
  - http://www.microsoft.com/france/mspress/default.asp?url=/france/mspress/ouvrage.asp?OuvrageID=1192
- Livre blanc sur la sécurité .NET Framework
  - http://www.microsoft.com/france/technet/themes/secur/info/info.asp?mar=/france/technet/themes/secur/info/20020612_fsnetsec.html
- Réaction à l'article du Monde « la tentation de Microsoft »
  - L'emmenant plus haut, le diable lui montra en un instant tous les royaumes de l'univers et lui dit : 'Je te donnerai tout ce pouvoir et la gloire de ces royaumes, car elle m'a été livrée, et je la donne à qui je veux'
  - http://www.microsoft.com/france/securite/entreprises/palladium/lettre_ouverte.asp

Dernières vulnérabilités
Infos Microsoft (4/4)

- **Microsoft publie des guides de configuration Windows 2000 Server**
  - **http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/prodtech/Windows/SecWin2k/Default.asp**
  - **http://www.microsoft.com/downloads/details.aspx?FamilyID=9964cf42-e236-4d73-aef4-7b4fdc0a25f6&DisplayLang=en**

- **Support NT4 : du nouveau**
  - **1er juillet 2002 : NT4 n'est plus disponible à la vente, y compris pour les OEM**
  - **1er juillet 2003 : NT4 n'est plus proposé aux intégrateurs**
  - **1er janvier 2004 : plus de correctifs hors sécurité**
  - **1er janvier 2005 : arrêt définitif du produit**

Dernières vulnérabilités
Autres avis (1/2)

EdelWeb

- Le CD d'installation de Windows 2000 permet d'ouvrir une Recovery Console sur un système XP sans mot de passe (quel que soit le paramétrage système)
  - J'ai testé : ca marche !
  - http://www.briansbuzz.com/w/030213/
- Outil WaveLock pour interdire les réseaux sans fil sous Windows 2000/XP
  - Gratuit
  - http://securewave.com/products/free_utilities/wavelock.html
- Déni de service TS
  - Affecte Windows 2000 (au minimum)
  - Si MSGINA.DLL est ouvert en mode exclusif, aucun autre utilisateur ne peut se logguer
  - Lors de la tentative de connexion, l'option « redémarrer le serveur » apparaît

Dernières vulnérabilités
Autres avis (2/2)

EdelWeb

- XP AntiSpy
  - http://www.xp-antispy.de/
  - Peut-être le sujet d'une prochaine présentation à l'OSSIR …
- Mise à jour des guides de sécurisation Windows XP de la NSA
  - 6 février 2003
- HFNetChk Pro 4.0
  - http://www.shavlik.com/

Questions / réponses

EdelWeb

- **Questions / réponses**
- **JSSI le 3 avril 2003**
- **Date de la prochaine réunion :**
  - **Lundi 12 mai 2003**
  - **Nous recherchons des sujets**
  - **Nous recherchons des salles**