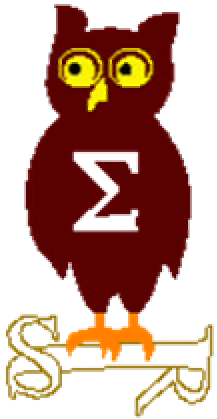
EdelWeb

OSSIR
Groupe Sécurité Windows

Réunion du 7 juillet 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 02/06/2003**
  - **MS03-020 Patch cumulatif pour IE**
    - **Affecte : IE 5.01, 5.5, 6.0**
    - **Cause : "buffer overflow" dans l'attribut "TYPE"**
    - **Exploit :**
      - **<object type="[/x64]AAAAAAAAAAAAAAAA">Test</object>**
    - **Autre vulnérabilité corrigée**
      - **"Bypass" des zones de sécurité lorsque le nombre de téléchargements simultanés dépasse la centaine**
  - **MS03-021 Contrôle ActiveX autorisant la manipulation de la "Media Library"**
    - **Affecte : Windows Media Player 9**
    - **Cause : bogue dans l'outil d'affichage des contrôles personnalisés en mode Web**
    - **Exploit : manipulation la librairie multimédia de l'utilisateur par tout contenu Windows Media**

Dernières vulnérabilités
Avis Microsoft (2/2)

- **MS03-022 Buffer overflow dans un filtre ISAPI**
  - **Affecte : Windows Media Services (Windows 2000)**
  - **Cause : filtre de journalisation "nsiislog.dll"**
  - **Exploit : exécution de code dans le contexte IWAM**

- **Re-releases**
  - **Aucune**

Dernières vulnérabilités
Infos Microsoft (1/2)

- Ouvrage "Improving Web Application Security: Threats and Countermeasures"
  - http://msdn.microsoft.com/library/en-us/dnnetsec/html/ThreatCounter.asp
- "Development Impacts of Security Changes in Windows Server 2003"
  - http://msdn.microsoft.com/library/en-us/dncode/html/secure06122003.asp
- Remplacement de ISM.DLL
  - Affecte : IIS 4.0 et 5.0
  - La nouvelle DLL ne nécessite plus les droits SYSTEM
  - http://support.microsoft.com/?id=331834

Dernières vulnérabilités
Infos Microsoft (2/2)

EdelWeb

- **Windows 2000 SP4**
  - Presque 1 an après le SP3 (11 mois)
  - 650 correctifs + USB 2.0, 802.1x …
  - Il y aura un SP5 avant la fin du support (31 mars 2005)

- **Windows 2003 SP1**
  - Attendu pour décembre
  - Inclura un outil de configuration automatique basé sur un fichier XML
    - Arrêt des services inutiles en fonction du rôle serveur
    - Fermeture des ports inutiles
  - Intègre la problématique Exchange, SQL, etc.

Dernières vulnérabilités
Autres avis (1/3)

- **Vulnérabilité dans le rendu des dossiers FTP par IE**
  - **Affecte : IE 5.01, 5.5 et 6.0**
  - **Exploit :**
    - **ftp://%3cimg%20src%3d%22%22%20onerror%3d%22alert%28document%2eURL%29%22%3e.example.com/**

    devient

    - **<H1>FTP root at <img src="" onerror="alert(document.URL)"> </H1>**
- **Déni de service via ICMPv6**
  - **Affecte : Windows 2000 / XP / 2003 avec IPv6**
  - **Exploit : http://www.securityfocus.com/bid/7788**
- **Récupération de cookies via le tag "about:"**
  - **Affecte : IE 5.0, 6.0**
  - **Exploit : http://security.novappc.com/nsrg-05-9/nsrg-05-9.txt**

Dernières vulnérabilités
Autres avis (2/3)

- Fuite d'information dans certains drivers réseau Windows 2003
  - Affecte :
    - VIA Rhine II Compatible network card
    - AMD PCNet family network cards
  - Exploit : http://www.nextgenss.com/advisories/etherleak-2003.txt
- Exécution de scripts en zone locale via les messages d'erreur
  - Affecte : IE 5.01, 5.5, 6.0
  - Exploit :
    - res://shdoclc.dll/404_HTTP.htm#http://site.com/file.html
  - Crédit : http://security.greymagic.com/adv/gm014-ie/
- XSS via fichiers XML invalides
  - Affecte : IE 5.5 et IE 6.0
  - Exploit :
    - http://host.with.unparsable.xml.file/flaw.xml?<script>alert(document.cookie) </script>
  - Crédit : http://security.greymagic.com/adv/gm013-ie/

Dernières vulnérabilités
Autres avis (3/3)

- **Buffer overflow dans IE**
  - Exploit :
    - <script> wnd=open("about:blank","","");
      wnd.moveTo(screen.Width,screen.Height);
      WndDoc=wnd.document; WndDoc.open(); WndDoc.clear();
      buffer=""; for(i=1;i<=127;i++)buffer+="X"; buffer+="DigitalScream";
      WndDoc.write("<HR align='"+buffer+"'>");
      WndDoc.execCommand("SelectAll");
      WndDoc.execCommand("Copy"); wnd.close(); </script>
- **Vulnérabilité Commerce Server 2002**
  - Mot de passe dans
    - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Commerce Server

Questions / réponses

EdelWeb

- **Questions / réponses**
- **Date de la prochaine réunion :**
  - **Septembre 2003 (date non fixée)**
  - **1 intervenant pressenti**
    - **Cyril VOISIN (Microsoft France) sur NGSCB**
- **N'hésitez pas à proposer des sujets et des salles**