EdelWeb

OSSIR
Groupe Sécurité Windows

Réunion du 5 juillet 2004

Revue des dernières vulnérabilités Microsoft

Nicolas RUFF

nicolas.ruff@edelweb.fr

Dernières vulnérabilités
Avis Microsoft (1/1)

EdelWeb

- **Avis de sécurité Microsoft depuis le 07/06/2004**
  - **MS04-016 Déni de service via DirectPlay**
    - **Affecte : DirectX 7+ (Windows 2000 SP2, XP, 2003)**
    - **Exploit : DoS**
    - **Source : John Lampe / Tenable Security**
  - **MS04-017 Déni de service via Crystal Reports**
    - **Affecte : Visual Studio .NET 2003, Outlook 2003 avec Business Contact Manager, Microsoft Business Solutions CRM 1.2**
    - **Exploit : DoS et fuite d'information**
    - **Source : Business Objects**
- **Mise à jour de bulletins**
  - **Juin 2004 :**
    - **MS04-011 (problème NT4 en version chinoise)**

Dernières vulnérabilités
Infos Microsoft (1/2)

EdelWeb

- ISA Server SP2
  - http://www.microsoft.com/downloads/details.aspx?FamilyID=c8d3d98b-1cd4-406a-a04a-2aa2547d09a3&DisplayLang=en
- "L'informatique de confiance" : bilan de l'année 2003
  - http://www.microsoft.com/france/securite/twc/default.mspx
- Téléchargez les CD Sécurité Microsoft
  - http://www.microsoft.com/france/securite/protection/cdrom.asp
- Antivirus Microsoft : ça se précise
  - "Microsoft on Track to Offer Anti-Virus Software"
    - http://www.reuters.com/newsArticle.jhtml?storyID=5429092
  - "Paid Microsoft Anti-Virus Subscription Service in the Works?"
    - http://www.entmag.com/news/article.asp?EditorialsID=6272

Dernières vulnérabilités
Infos Microsoft (2/2)

EdelWeb

- **Roadmap Microsoft**
  - **http://techrepublic.com.com/5100-6265_11-5211742.html?tag=e019**
  - **2004 :**
    - **Longhorn Server Beta 1**
  - **2006 :**
    - **Longhorn Server Beta 2**
    - **Longhorn Workstation**
    - **Windows 2003 SP2**
  - **2007 :**
    - **Longhorn Server Final**
  - **2008 :**
    - **Longhorn SP1 (les bugs sont déjà inclus ☺)**
  - **2009 :**
    - **Longhorn SP2**

Dernières vulnérabilités
Autres avis (1/7)

EdelWeb

- **Attaques Web de grande ampleur**
  - **Attaque SCOB**
    - **Des serveurs "grand public" ont été compromis par la faille LSASS**
    - **Le "footer" a été remplacé par un script malveillant**
    - **Les utilisateurs d'IE ont été infectés par un Trojan**
    - **Références**
      - **http://www.microsoft.com/security/incident/download_ject.mspx**
      - **http://www.lurhq.com/berbew.html**
    - **Ex. faire une recherche Google sur "function gc099"**
  - **Attaque sur les mots de passe bancaires**
  - **Le CERT-IST recommande de ne pas utiliser IE**
  - **Workaround : Q870669 (désactivation ADODB)**

Dernières vulnérabilités
Autres avis (2/7)

EdelWeb

- **Ver Cabir sur les téléphones portables**
  - Ver pour Symbian OS
  - Preuve de concept :
    - se propage par Bluetooth
    - ne possède pas de charge finale

- **Étude Deloitte & Touche sur la sécurité informatique**
  - Budgets en baisse partout
  - Nombre d'attaques en hausse
  - Problèmes viraux principalement (perçus et réels)
  - http://www.deloitte.com/dtt/cda/doc/content/GFSISE.pdf

- **Nouveau site de failles IE**
  - http://iebug.com/
  - Maintenu par Liu Die Yu

- **Googling NT (les failles ASP.NET)**
  - allinurl: "trace.axd"
  - allinurl: "web.config"
  - allinurl: "aspx.cs" for C# source
  - allinurl: "aspx.vb" for VBS source

Dernières vulnérabilités
Autres avis (3/7)

EdelWeb

- **Bogues IE**
  - **Technique baptisée "Cœlacanthe"**
    - **"0-day" exploité par le Malware "180-Solutions"**
    - **Problème dans le décodage des caractères**
      - **Soit dans le header "Host:"**
      - **Soit dans l'adresse DNS renvoyée**
        - **Ne nécessite pas forcément le contrôle d'un serveur DNS**
        - **Ex. <script>alert()<% 2Fscript>.e-gold.com'>foo**
        - **Cf. http://www.securityfocus.com/bid/10554**
    - **Exploit :**
      - **Permet de l'exécution de script en zone poste de travail**
      - **Permet du spoofing SSL via redirection**
      - **Démo :**
        - **http://www.malware.com/gutted.html**
    - **Affecte :**
      - **IE mais aussi Mozilla**

Dernières vulnérabilités
Autres avis (4/7)

EdelWeb

- **Abus des CLSID**
  - **Affecte :**
    - **Explorateur Windows via IE**
  - **Exploit :**
    - **<a href=.{3E9BAF2D-7A79-11d2-9334-0000F875AE17}>**
    - **Lance NetMeeting**
    - **http://www.freewebs.com/roozbeh_afrasiabi/xploit/execute.htm**
- **Bogue Outlook 2003**
  - **Le lecteur Windows Media n'est pas soumis aux restrictions de sécurité**
  - **Exploit :**
    - **http://www.malware.com/rockIT.zip**

Dernières vulnérabilités
Autres avis (5/7)

EdelWeb

- **Bogue OE**
  - **MIME-Version: 1.0**
  - **Content-Type: text/plain;**
  - **charset="Windows-1252"**
  - **Content-Transfer-Encoding: 7bit**
  - **<img><object data=http://www.malware.com>**
  - ***ou***
  - **~object data=3D"http://www.seductiveones.~biz/easy/orrorr/sock/page.~php"~=20**

Dernières vulnérabilités
Autres avis (6/7)

EdelWeb

- **Bugtraq**
  - **Déni de service via une feuille de style**
    - **Affecte : IE**
    - **Exploit : http://www.zeepost.nl/~henkie/index.html**
    - **Source : http://www.securityfocus.com/bid/10382**
  - **Masquage d'URL**
    - **Affecte : IE + Opera**
    - **Exploit : "http://[site_confiance]%2F%20%20%20.[site_malicieux]/"**
    - **Source : http://www.securityfocus.com/bid/10517/**
    - **Variante affectant IE**
      - **"http://example%2fwww.example.example.org"**
      - **Permet l'exécution de scripts en zone PdT**
    - **Source : http://www.securityfocus.com/bid/10579/**

Dernières vulnérabilités
Autres avis (7/7)

EdelWeb

- **Variante des failles MS-ITS utilisant l'entête "location"**
  - **Affecte : IE**
  - **Exploit : 'Location: URL:ms-its:C:\WINDOWS\Help\iexplore.chm::/iegetsrt.htm"**
- **Accès aux fichiers locaux via une URL malformée**
  - **Affecte : IE**
  - **Exploit : "URL:" + nom de fichier**
  - **Source : http://www.securityfocus.com/bid/10472/**
- **Contournement des zones de sécurité via un dialogue modal dans une IFRAME**
  - **Affecte : IE**
  - **Exploit : N/D**
  - **Source : http://www.securityfocus.com/bid/10473/**

Dernières vulnérabilités
Nouveaux outils (1/1)

EdelWeb

- **WiSSH : RDP sur SSH**
  - **http://www.wissh.com/**

Questions / réponses

EdelWeb

- **Questions / réponses**
- **Date de la prochaine réunion**
  - **Pas de réunion en août**
  - **Septembre 2004**
- **N'hésitez pas à proposer des sujets et des salles**