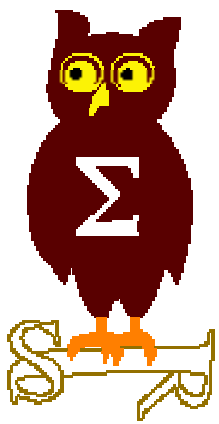
OSSIR
Groupe Sécurité Windows

Réunion du 9 janvier 2006



Revue des dernières vulnérabilités Microsoft

Nicolas RUFF

EADS-CCR

nicolas.ruff@eads.net

Dernières vulnérabilités
Avis Microsoft (1/4)

- (Avis de sécurité Microsoft depuis le 12 décembre 2005)

- Décembre 2005
  - MS05-054 (Q911302) : patch cumulatif pour IE
    - Affecte : IE 5.01 SP4, IE 5.5 SP2, IE 6.0 SP1
    - Exploit : disponible dans la nature avant le patch
      - Méthode Window()
    - Crédit : Will Dormann (CERT/CC), Andreas Sandblad / Jakob Balle (Secunia)

  - MS05-055 : vulnérabilité dans le noyau Windows
    - Affecte : Windows NT4, Windows 2000
      - Corrigé silencieusement dans Windows XP
    - Exploit :
      - "Heap overflow" dans le noyau Windows (exploitable)
      - Disponible sur le site XFocus
    - Crédit : Derek Soeder (eEye)

Dernières vulnérabilités
Avis Microsoft (2/4)

- **Janvier 2006**
  - **MS06-001 (Q912840) "faille WMF"**
    - **Affecte :**
      - **Toutes les versions Windows depuis 3.0**
        - **Composant contenant le "bug" : GDI32.DLL**
        - **"It's not a bug, it's a feature" ™ : SetAbortProc() peut contenir du code …**
      - **Exploitable via IE et Outlook (y compris XP SP2)**
        - **Composant "Windows Picture and Fax Viewer" (shimgvw.dll)**
      - **Exploitable via Lotus Notes**
        - **http://www.nist.org/nist_plugins/content/content.php?content.25**
    - **Exploit :**
      - **Exécution de code via un fichier .WMF**
      - **Découvert et exploité "dans la nature"**
    - **Crédit :**
      - **Hubbard Dan / Websense (?)**

Dernières vulnérabilités
Avis Microsoft (3/4) – faille WMF

- **Beaucoup d'encre a coulé**
  - http://sunbeltblog.blogspot.com/2005/12/new-wmf-exploit-confirmed-in-spam.html
  - http://isc.sans.org/diary.php?storyid=994
  - http://blogs.securiteam.com/index.php/archives/167
  - http://www.frsirt.com/bulletins/3344

- **Patchs non officiels**
  1. Désactiver shimgvw.dll
  2. Patch binaire par Ilfak Guilfanov
     - http://www.hexblog.com/2005/12/wmf_vuln.html

- **Polémique**
  - Fallait-il publier l'exploit le 31 décembre ?
    - http://www.f-secure.com/weblog/archives/archive-012006.html#00000758

- **Sondage ISC**
  - "Was the release of the 2nd generation WMF exploit on Dec 31st 2005 irresponsible ?"
    - 39 % =>Yes, I 'd like to see the authors brought to justice
    - 22 % =>Yes, they made the world a worse place
    - 28 % =>No, the bad guys had already equal ammunition
    - 10 % =>No, I believe the ends did justify the means
    - Total Answers: 797

Dernières vulnérabilités
Avis Microsoft (4/4)

- Autres bulletins
  - 1 bulletin critique affectant Windows
  - 1 bulletin critique affectant Exchange et Office
  - 1 mise à jour pour WU et SUS
  - 3 mises à jour pour MU et WSUS

Advisories

- Q912920 Virus Sober.Z

Révisions

- MS05-011
  - Version 1.1 : problème identifié lié au patch (Q896427)
- MS05-050
  - Version 2.0 : nouvelle version du patch

Dernières vulnérabilités
Infos Microsoft (1/1)

- **Microsoft retire le support graphique en mode noyau dans Vista**
  - **http://addxorrol.blogspot.com/2005/12/microsoft-is-moving-gui-code-back-out.html**
  - **http://www.techworld.com/news/index.cfm?RSS&NewsID=5002**
  - **Introduit dans NT4 pour des raisons de performance**
  - **Les drivers graphiques sont sources de trop de "BSoD"**

Dernières vulnérabilités
Autres avis (1/5) - failles

- **Cross-site scripting via import de CSS en chaine**
  - **Affecte : IE 6 SP1**
  - **Exploit : http://secunia.com/advisories/17564/**
    - **relativement difficile à exploiter "dans la nature"**
  - **Crédit :**
    - **http://www.hacker.co.il/security/ie/css_import.html**

- **"Heap overflow" dans tous les produits Symantec**
  - **Affecte : tous les produits Symantec**
  - **Exploit : "heap overflow" dans le traitement des fichiers RAR par "dec2rar.dll"**
  - **Crédit : Alex Wheeler**

  - **Pas de solution officielle !**

Dernières vulnérabilités
Autres avis (2/5) - failles

- **DoS IIS**
  - **Affecte : IIS 5.1 (Windows XP)**
  - **Exploit :**
    - **http://www.example.com/_vti_bin/.dll/*\~0**
    - **Nécessite un répertoire en exécution pour les scripts et les programmes**
    - **http://ingehenriksen.blogspot.com/2005/12/microsoft-iis-remote-dos-dll-url.html**
  - **Pas de correctif pour le moment**
- **3 DoS IE (pour la collection)**
  - **Affecte : IE toutes versions**
  - **Exploits :**
    - **<table datasrc=".">**
    - **</samp> </colgroup> <font> <menu> <code> <var> <sub> <h2> </fieldset> </kbd> </frameset> </ins> </map> </noframes> </isindex> </code> </title> </del> </var> <isindex> <i>**
    - **<acronym> <dd> <h5> <applet> </caption> </applet> </h1>**

Dernières vulnérabilités
Autres avis (3/5) – virus et spywares

- **Le spyware Apropos utilise des techniques de "rootkit" très avancées**
  - **http://www.eweek.com/article2/0,1759,1897728,00.asp**
- **Un autre ver de script affecte le portail Xanga**
  - **http://blogs.securiteam.com/index.php/archives/166**

Dernières vulnérabilités
Autres avis (4/5)

- **Un bug dans Microsoft Small Business Server provoque l'émission de plusieurs millions de messages**
  - **http://www.theregister.co.uk/2005/12/10/server_bug_cripples_dublin_law_firms/**
- **Une curieuse étude Sophos**
  - **16,000 nouveaux virus en 2005**
  - **Les utilisateurs domestiques devraient se tourner vers Mac**
  - **http://www.pcpro.co.uk/news/81079/nearly-16000-new-viruses-this-year-says-sophos.html**
- **Intel prévoit les premières puces à TPM intégré en 2008-2009**
  - **http://www.theregister.co.uk/2005/12/09/intel_anti-rootkit_chip/**
- **D'après le FBI, le cyber-terrorisme n'est pas pour demain**
  - **http://www.enterprise-security-today.com/story.xhtml?story_id=40010**

Dernières vulnérabilités
Autres avis (5/5)

- Il est possible de contourner les GPOs
  - Utiliser la commande "Run As …" ou "runas /noprofile"

Questions / réponses

- **Questions / réponses**
- **Date de la prochaine réunion**
  - **AG Mardi 10 janvier 2006**
  - **Lundi 13 février 2006**
- **N'hésitez pas à proposer des sujets et des salles**