OSSIR
Groupe Sécurité Windows

Réunion du 15 janvier 2007

Revue des dernières vulnérabilités Microsoft

Cette veille est réalisée par les coanimateurs du groupe Windows

EdelWeb

Olivier REVENU
EdelWeb
olivier.revenu@edelweb.fr

Nicolas RUFF
EADS-CCR
nicolas.ruff@eads.net

Dernières vulnérabilités
Avis Microsoft (1/12)

- **Préalable**
  - **La criticité indiquée pour chaque avis est donnée selon l'échelle Microsoft, à savoir**

    Faible
    - **Une vulnérabilité dont l'exploitation est très difficile ou dont l'impact est minimale**

    Modéré
    - **L'exploitabilité est limitée par des facteurs comme la configuration par défaut non vulnérable ou est très difficile à réaliser**

    Important
    - **Une vulnérabilité dont l'exploitation aura pour impact l'atteinte à la confidentialité, l'intégrité ou la disponibilité des données des utilisateurs, voir l'intégrité ou la disponibilité du système**

    Critique
    - **Une vulnérabilité dont l'exploitation peut permettre la propagation d'un vers Internet sans action de l'utilisateur**

  - **Les exploits indiqués pour chaque avis sont ceux connus publiquement à la date de cette présentation**

Dernières vulnérabilités
Avis Microsoft (2/12)

- **Correctifs de Décembre 2006**

Bulletin	Faille	Affecte	Détails	Exploit
MS06-072	**Patch cumulatif pour IE** (Jakob Balle & Carsten Eiram / Secunia Sam Thomas / ZDI Yorick Koster / ITsec Security)	**IE toutes versions supportées sauf IE 7**	**4 vulnérabilités** **CVE-2006-5577** **CVE-2006-5578** **CVE-2006-5579** **CVE-2006-5581** **→Exécution de code** **→Divulgation de contenu**	**Non**
MS06-073	**Vulnérabilité dans un ActiveX Visual Studio 2005** (ZDI)	**Visual Studio 2005**	**WMI Object Broker (wmiscriptutils.dll)** **CVE-2006-4704**	**0day**

Dernières vulnérabilités
Avis Microsoft (3/12)

Bulletin	Faille	Affecte	Détails	Exploit
MS06-074	Vulnérabilité SNMP (EADS-CCR)	Windows toutes versions supportées sauf Vista	Boundary error dans le service →exécution de code à distance sous SYSTEM	Oui (payant)
MS06-075	Elévation de privilèges (n/d)	Windows XP SP2, Windows 2003 "Gold"	Fichier "manifest" malformé	Non
MS06-076	Patch cumulatif pour Outlook (n/d)	Windows toutes versions supportées sauf Vista	Exécution de code via un fichier WAB malformé (CVE-2006-2386)	Non

Dernières vulnérabilités
Avis Microsoft (4/12)

Bulletin	Faille	Affecte	Détails	Exploit
MS06-077	**Compromission d'un serveur RIS à distance** (Nicolas RUFF / EADS-CCR)	**Windows 2000 SP4**	**TFTP en écriture avec les droits SYSTEM**	**Trivial**
MS06-078	**Vulnérabilités multiples dans Windows Media** Player (n/d)	**Windows Media Player toutes versions supportées sauf la 11**	**Overflow dans le traitement des fichiers ".ASF" (CVE-2006-4702)** **Overflow dans le traitement des fichiers ".ASX" (CVE-2006-6134)** **Note : ce patch n'était pas prévu pour décembre initialement**	**0day**

Dernières vulnérabilités
Avis Microsoft (5/12)

- **Un patch Office Mac sorti par erreur**
  - **http://www.microsoft.com/mac/autoupdate/description/AUOffice20041131EN.htm**
- **De bonnes analyses des patches :**
  - **http://www.eeye.com/research/html/newsletters/alert/pub/AL20061212.html**
  - **http://portal.spidynamics.com/blogs/msutton/archive/2006/12/12/-Microsoft-Black-Tuesday-_2D00_-December-2006.aspx**
  - **http://isc.sans.org/diary.php?date=2006-12-13**

Dernières vulnérabilités
Avis Microsoft (6/12) - Synthèse

IMPACT MS	VECTEUR D'EXPLOITATION PREMIER Internet	LAN	Utilisateur
Exécution de code à distance		SNMP (074) RIS (077)	IE (072) VISUAL STUDIO (073) OUTL EXPRESS (076) MEDIA PLAYER (078)
Élévation de privilèges			CSRSS (075)
Usurpation de contenu			
Déni de service			
Divulgation d'informations			

Dernières vulnérabilités
Avis Microsoft (7/12)

- **Bulletins du mois de janvier 2007**
  - **Au début :**
    - **3 bulletins Windows allant jusqu'à "critique"**
    - **1 bulletin Windows + Visual Studio "important"**
    - **1 bulletin Windows + Office "important"**
    - **3 bulletins Office allant jusqu'à "critique"**
  - **Puis :**
    - **1 bulletin Windows "critique"**
    - **3 bulletins Office allant jusqu'à "critique"**

Dernières vulnérabilités
Avis Microsoft (8/12)

- **Bulletins définitifs pour le mois de janvier**

Bulletin	Faille	Affecte	Détails	Exploit
MS07-001	**Vulnérabilité dans le correcteur grammatical brésilien** (n/d)	**Office 2003**	**Exécution de code via un document malformé**	**Oui**
MS07-002	**Vulnérabilités Excel multiples (x5)** (Jeff Gennari / CERT, Jie Ma / Fortinet, NSFocus, Greg MacManus / iDefense)	**Excel toutes versions (y compris Mac) sauf 2007**	**Exécution de code via un document malformé**	**Non**

Dernières vulnérabilités
Avis Microsoft (9/12)

Bulletin	Faille	Affecte	Détails	Exploit
MS07-003	**Vulnérabilités Outlook multiples (x3)** (Lurene Grenier / Sourcefire, Stuart Pearson / Computer Terrorism)	**Outlook toutes versions (sauf 2007)**	**Exécution de code et déni de service**	**Oui (DoS)**
MS07-004	**Vulnérabilité dans le traitement des fichiers VML** (Jospeh Moti à travers iDefense)	**IE 5.01 -> 7.0 sauf Vista (!)**	**Exécution de code (Cf. MS06-055)**	**Oui**

Dernières vulnérabilités
Avis Microsoft (10/12) - Synthèse

IMPACT MS	VECTEUR D'EXPLOITATION PREMIER Internet	LAN	Utilisateur
Exécution de code à distance			**OFFICE (001)** **EXCEL (002)** **OUTLOOK (003)** **VML (004)**
Élévation de privilèges			
Usurpation de contenu			
Déni de service			**OUTLOOK (003)**
Divulgation d'informations			

Dernières vulnérabilités
Avis Microsoft (11/12)

- **Advisories**
  - **Q927709 : MS06-073 (Visual Studio 2005 ActiveX)**
  - **Un troisième "0day" Word, publié dans la nature !**
    - **→ http://www.milw0rm.com/exploits/2922**

Dernières vulnérabilités
Avis Microsoft (12/12)

- **Révisions**
  - **MS06-012**
    - **Version 1.5 : mise à jour de la liste des fichiers**
  - **MS06-016**
    - **Version 1.3 : mise à jour de la liste des fichiers**
  - **MS06-071**
    - **Version 1.2 : erreur de syntaxe dans le paramètre "/log"**
  - **MS06-072**
    - **Version 1.1 : mise à jour pour les systèmes non-x86**
  - **MS06-078**
    - **Version 2.0 : re-publication pour les versions coréennes**
    - **Version 2.1 : mise à jour du FAQ**
  - **MS07-002**
    - **Version 1.1 : incompatibilités détectées**
  - **MS07-004**
    - **Version 1.1 : un *reboot* n'est pas toujours nécessaire**

Dernières vulnérabilités
Infos Microsoft (1/2)

- **Microsoft commence à travailler sur l'API noyau Vista …**
  - **… demandée par les éditeurs antivirus**

  →http://www.microsoft.com/security/windowsvista/fathi.mspx

- **Dans Windows Vista, tout appel à l'UEF sera remonté à Microsoft via Windows Error Reporting (WER)**
  - **Cf. présentation de Mark Russinovitch**

  →http://www.microsoft.com/emea/itsshowtime/sessionh.aspx?videoid=340

- **IE7 passe la barre des 100 million**
  - **http://blogs.msdn.com/ie/archive/2007/01/12/100-million-ie7-installations.aspx**
  - **Une part de marché estimée à 25%**
  - **Est devenu une mise à jour optionnelle sur WindowsUpdate**

Dernières vulnérabilités
Infos Microsoft (2/2)

- **Sorties**
  - **Q917021**
    - **Un hotfix pour ne plus broadcaster ses réseaux WiFi préférés !**
  - **Windows 2003 SP2 RC1**
  - **Visual Studio 2005 SP1**
    - **Indispensable pour utiliser Vista à son maximum … (ex. ASLR)**
    - **Mais personne n'est parfait**
      - **→ http://msdn2.microsoft.com/en-us/vstudio/aa948853.aspx?lcid=1033**

Dernières vulnérabilités
Autres avis (1/9) – failles

- **Le premier bug Vista**
  - **Affecte : Windows 2000, XP, 2003, Vista**
  - **Exploit :**
    - **Elévation de privilèges vers SYSTEM**
    - **Plusieurs erreurs**
      - **FreePhi() "double free()"**
      - **NtRaiseHardError() "memory disclosure«**

→http://www.determina.com/security.research/vulnerabilities/csrss-harderror.html

```
#include <windows.h>
int main(void){
    int i;
    char bug1 [] ="\\??\\XXXX";
    for(i = 0; i < 10; i ++)
          MessageBox(0, bug1, bug1,
       MB_SERVICE_NOTIFICATION);
}
```

Dernières vulnérabilités
Autres avis (2/9) – failles

- **Un "0day" Vista vendu $50,000 ?**
  - **Rumeur répandue par Trend Micro**
  - **Aucune information disponible**

- **Le challenge "officiel"**
  - **$8,000 par faille Vista ou IE7 exploitable à distance**
  - **+ $2,000 à $4,000 pour l'exploit**

  →http://labs.idefense.com/vcp/challenge.php#more_q1+2007%3A+vulnerability+challenge

- **Janvier : le mois des failles Apple**
  - **Failles et codes d'exploitation pour tout logiciel fonctionnant en environnement Mac OS X**
  - **Très médiatique**

- **De nombreuses failles dans la JVM Sun**
  - **Mettre à jour en version 1.5.10 rapidement !**
  - **Note : Java 6 est disponible**

    → http://java.sun.com/javase/6/

Dernières vulnérabilités
Autres avis (3/9) – failles

- **Faille dans Acrobat Reader**
  - **Affecte : Acrobat < 8**
  - **Exploit : http://site.com/example.pdf#script…**
  - **Baptisée "Universal XSS"**

- **Faille dans les drivers Intel Centrino 2200**
  - **Affecte : version 9.0.3.9**
  - **Exploit : corruption de la mémoire du noyau**
    - **Exécution de code possible**

- **Faille dans le traitement des fichiers MIDI**
  - **Affecte : Windows Media Player 6 -> 10**
  - **Exploit : déni de service (?)**

  → http://milw0rm.com/exploits/2935

Dernières vulnérabilités
Autres avis (4/9) – failles

- **Faille dans Project Server**
  - **Affecte : Microsoft Project Server 2003**
  - **Exploit : publication du mot de passe en clair dans la requête POST sur la page "logon/pdsrequest.asp"**

- **Faille dans Event Viewer**
  - **L'interprétation du "%1", "%2", … est récursive**
  - **Exploit : "net send <cible> %2"**

- **Une "feature" intéressante dans les portables Acer**
  - **Le contrôle ActiveX "LunchApp.ocx" permet à une page Web de lancer n'importe quel exécutable sur le poste local !**

Dernières vulnérabilités
Autres avis (5/9) – failles Web

- **Opera 9.1 intègre une protection anti-phishing**
  - **Basé sur GeoTrust et Phishtank**
  - **Rappel :**
    - **Firefox 2 utilise Google AntiTrust**
    - **IE 7 utilise "URL Reputation Web Service" (via MSN)**
    - **Safari 3 aura aussi une protection …**

- **Nouvelle attaque : le "DNS Pinning"**
  - **Principe :**
    - **"Attacker.org" répond aux requêtes DNS du client avec une IP interne "de confiance" (obtenue par scan JavaScript)**

  → http://shampoo.antville.org/stories/1451301/

Dernières vulnérabilités
Autres avis (6/9) – virus et spywares

- **Le site Web de Asus infecté par des spywares**
  - → **http://www.heise-security.co.uk/news/82643**
- **Un ver se propage en exploitant une faille dans les produits Symantec**
  - **Port TCP/2967**
  - → **http://research.eeye.com/html/alerts/AL20061215.html**
- **Un ver se propage via Skype**
  - **Aucune innovation technique (cf. vers Yahoo, MSN, …)**
  - **Nécessite une confirmation utilisateur**
  - **Techniquement intéressant**
  - → **http://www.websense.com/securitylabs/blog/blog.php?BlogID=102**
- **Un "password stealer" ciblant Skype ("PWS-JO")**
  - **Vol de minutes SkypeOut ?**
  - **SPIT ?**
    - **(Spam over VoIP)**

Dernières vulnérabilités
Autres avis (7/9) – virus et spywares

- **"ILOVEYOU" réécrit en AppleScript**
  → **http://blog.info-pull.com/2006/12/26/applescript-even-easier-than-vbs-i/**

- **Les premiers sites de phishing en Flash**

- **Les ratés de l'anti-phishing**
  - **Des informations personnelles se retrouvent parfois dans les blacklists !**

  → **http://sb.google.com/safebrowsing/update?version=goog-black-url:1:1**

- **Les prévisions de WebSense pour 2007**
  - **Web 2.0 security issues continue to escalate**
    - **User-created content**
    - **Social Networks**
    - **SOA / Web Services**
  - **Criminal Underground Economy / Zero-day Market Increases**
  - **Anti-Phishing Toolbar Exploits**
  - **Enhanced Concealment of Data**
  - **BOT Evolution**

  → **http://www.websense.com/securitylabs/blog/blog.php?BlogID=99**

Dernières vulnérabilités
Autres avis (8/9)

- **Une astuce intéressante**
  - **"win.com cmd.exe" lance un CMD**
  - **"win.com" est exécutable par IUSR_xxx**

- **La FSF lance BadVista.org**
  - **"Vista est un régression pour le consommateur et contient des chevaux de Troie"**
- **Ils n'ont pas forcément tort !**
  - **Vista ne serait qu'un énorme lecteur de DVDs …**

  → http://www.cs.auckland.ac.nz/~pgut001/pubs/vista_cost.txt
- **Et la NSA aurait participé activement au développement**

  → http://silicon.fr/fr/silicon/news/2007/01/10/secours-nsa-a-particip-d

- **Le gouvernement américain va imposer le cryptage intégral de tous les disques dans les administrations**

  → http://www.full-disk-encryption.net/fde_govt.html

Dernières vulnérabilités
Autres infos (9/9)

- **Et pendant ce temps là sur la mailing liste de l'OSSIR**
  - **Liste SUR**
    - **Squid Reverse proxy**
    - **Comment bloquer une adresse ip ?**
    - **Vive l'administration électronique !**
    - **Sécurité des suites bureautique**
  - **Liste NT**
    - **RCSR, firefox et ses passwords**

Questions / réponses

- **Questions / réponses**
- **Date de la prochaine réunion**
  - **Assemblée Générale le 16 janvier 2007**
  - **Prochaine réunion le 5 février 2007**
- **N'hésitez pas à proposer des sujets et des salles**
- **Et surtout …**
  - **Bonne année à tous !**