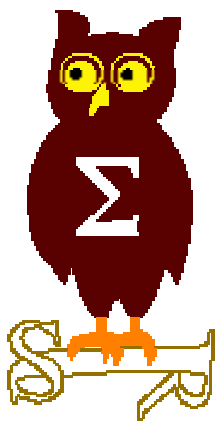
EdelWeb

OSSIR
Groupe Sécurité Windows

Réunion du 10 juillet 2006



Revue des dernières vulnérabilités Microsoft

Olivier REVENU

olivier.revenu@edelweb.fr

Dernières vulnérabilités
Avis Microsoft (1/8)

EdelWeb

- **Avis de sécurité Microsoft depuis le 13 juin 2006**
  - **MS06-021 – Patch cumulatif pour Internet Explorer**
    - **Affecte : toutes versions de IE supportées**
    - **Exploit : 8 failles exploitables à distance pour**
      - **Exécuter du code à distance**
      - **Réaliser des attaques de phishing (window.open et URL Bar)**
      - **Divulguer des fichiers locaux (directive @import – CSSXSS – PoC Google Desktop)**
    - **Vecteur : page web, email HTML**
    - **Crédit : multiples**
  - **MS06-022 – Vulnérabilité dans le traitement des images ART**
    - **Affecte :**
      - **Windows 2000 SP0 avec support ART & SP4**
      - **Windows XP SP0 SP1 SP2**
      - **Windows 2003 SP0 SP1**
    - **Exploit : heap buffer overflow permettant d'exécuter du code lors de l'affichage d'une image ART malformée**
    - **Vecteur : page web, email HTML, image**
    - **Crédit : iDEFENSE**

Dernières vulnérabilités
Avis Microsoft (2/8)

- **MS06-023 – Vulnérabilité dans Microsoft Jscript**
  - Affecte : JScript 5.1, 5.5, 5.6
  - Exploit : corruption de la mémoire permet d'exécuter du code
  - Vecteur : page web, email HTML
  - Crédit : Microsoft

- **MS06-024 – Vulnérabilité dans le traitement des PNG par Media Player**
  - Affecte : Windows Media Player 7.1, 9, 10
  - Exploit : stack buffer overflow
  - Vecteur : skin WMZ, page web
  - Crédit : iDEFENSE

- **MS06-025 – Vulnérabilités dans les services de routage**
  - Affecte : Windows 2000 SP4, XP SP0/SP1/SP2, 2003 SP0/SP1
  - Exploit : buffer overflow dans RemoteAccess et RASMAN (credentials nécessaires pour XP SP2 et 2003)
  - Vecteur : requête RPC malformée
  - Crédit : NGS Software, Microsoft

Dernières vulnérabilités
Avis Microsoft (3/8)

- **MS06-026 – Vulnérabilité dans le traitement des fichiers WMF/EMF**
  - **Affecte : Windows 98, 98 SE, Me**
  - **Exploit : heap buffer overflow dans le moteur de rendu**
  - **Vecteur : page web, email HTML, image**
  - **Crédit : Symantec**

- **MS06-027 – Vulnérabilité dans Word à l'ouverture de documents malformés**
  - **Affecte : Office 2000/XP/2003, Works Suite 2000-2006**
  - **Exploit : buffer overflow faisant l'objet d'un 0day en juin**
  - **Vecteur : fichier word malformé, backdoor Ripgof.B**
  - **Crédit : ICST**

- **MS06-028 – Vulnérabilité dans PowerPoint à l'ouverture de documents malformés**
  - **Affecte : Office 2000/XP/2003, Office MAC 2004/X**
  - **Exploit : buffer overflow**
  - **Vecteur : fichier ppt malformé**
  - **Crédit : EADS CCR, Symantec, Fortinet**

Dernières vulnérabilités
Avis Microsoft (4/8)

EdelWeb

- **MS06-029 – Injection de script dans Exchange OWA**
  - Affecte : Exchange 2000 SP3 & Update Rollup, 2003 SP1/SP2
  - Exploit : XSS via balise HTML avec '\0' en argument
  - Vecteur : email HTML
  - Crédit : SEC Consult

- **MS06-030 – Vulnérabilités dans le driver MRXSMB.SYS**
  - Affecte : Windows 2000 SP4, XP SP0/SP1/SP2, 2003 SP0/SP1
  - Exploit : élévation de privilèges et déni de service
  - Vecteur : programme exécuté localement
  - Crédit : Ruben Santamarta (PoC dispo mais en désactivant EnforceWriteProtection)

- **MS06-031 – Spoofing du serveur dans l'authentification mutuelle RPC**
  - Affecte : Windows 2000 SP4
  - Exploit : man-in-the-middle (erreur de validation d'un service RPC de la part d'un client RPC)
  - Vecteur : requête RPC
  - Crédit : Symantec

Dernières vulnérabilités
Avis Microsoft (5/8)

EdelWeb

- **MS06-032 – Vulnérabilité dans le driver TCPIP.SYS**
  - **Affecte : Windows 2000 SP4, XP SP0/SP1/SP2, 2003 SP0/SP1**
  - **Exploit : buffer overflow entrainant un DoS ou l'exécution de code ring0 (nécessite RRAS et IPSourceRouting)**
  - **Vecteur : paquet IP malformé**
  - **Crédit : Andrey Minaev**

Re-release

- **MS06-011 DACLs des services Windows trop permissifs**
  - **Mise à jour des valeurs de registre pour la sécurité des services NetBT, RemoteAccess, et TCPIP**
  - **Date initiale : 16 mars 2006**
- **MS06-025 Vulnérabilités dans les services de routage**
  - **Correction des problèmes avec les connexions à distance utilisant des dial-up scripts**
  - **Date initiale : 27 juin 2006**

Dernières vulnérabilités
Avis Microsoft (6/8)

- **Advisories**
  - **Q912945 : Patch de compatibilité IE / ActiveX**
    - **Migration forcée vers le nouveau modèle ActiveX par MS06-021**
  - **Q914784 : MAJ protection noyau 64 bits (XP et 2003)**
  - **Q921365 : 0day dans Excel**
  - **Q921923 : PoC pour la vulnérabilité RASMAN (MS06-025)**
    - **Publiée dans Metasploit**
  - **Q919637 : 0day dans Word XP/2003**
    - **Corrigé par MS06-027**
- **Patch day Juillet 2006**
  - **4 bulletins de sécurité pour Windows (sévérité max : critique)**
  - **3 bulletins de sécurité pour Office (sévérité max : critique)**
  - **Mise à jour de MSRT**

Dernières vulnérabilités
Avis Microsoft (7/8)

EdelWeb

- **Révisions**
  - **MS06-011**
    - **Version 2.0 : mise à jour des valeurs par défaut dans la base de registre**
    - **Version 2.1 : précision sur Windows 2003 SP0**
  - **MS06-021**
    - **Version 1.1 : suppression des versions de Windows non supportées**
  - **MS06-024**
    - **Version 1.1 : précision sur WMP 9 + Windows 2000**
  - **MS06-025**
    - **Version 1.1 : MAJ de la Faq, problèmes de compatibilité avec les scripts de Dial Up**
    - **Version 1.2 : précisions sur entre RAS, RRAS et RASMAN**
    - **Version 2.0 : republication correction d'un problème de comptabilité**

Dernières vulnérabilités
Avis Microsoft (8/8)

EdelWeb

- **MS06-027**
  - **Version 1.1 : MAJ des remerciements**
  - **Version 1.2 : précisions sur Word 2003**
- **MS06-028**
  - **Version 1.1 : MAJ du fichier d'installation de PowerPoint 2003**
  - **Version 1.2 : MAJ sur les patch remplacés**
- **MS06-030**
  - **Version 1.1 : MAJ des remerciements**
- **MS06-032**
  - **Version 1.1 : précisions sur la désactivation de l'IP Source Routing**

Dernières vulnérabilités
Infos Microsoft (1/3)

- Sortie de Microsoft Antigen le 6 juin 2006
  - http://www.microsoft.com/presspass/press/2006/jun06/06-06AntigenPR.mspx
- WinFx devient ".NET Framework 3.0"
  - http://msdn.microsoft.com/winfx/
- Des changements profonds dans WinFS
  - http://blogs.msdn.com/winfs/
- Vista : "The Broken Windows Theory"
  - http://blogs.msdn.com/philipsu/archive/2006/06/14/631438.aspx
- Ajouter une licence Creative Commons sur un document Office
  - http://www.microsoft.com/downloads/details.aspx?familyid=113B53DD-1CC0-4FBE-9E1D-B91D07C76504&displaylang=en
- Le labo Open Source de Microsoft
  - http://port25.technet.com/

Dernières vulnérabilités
Infos Microsoft (2/3)

EdelWeb

- Evolution de la menace virale, mesurée via MSRT
  - http://www.microsoft.com/downloads/details.aspx?FamilyId=47DDCFA9-645D-4495-9EDA-92CDE33E99A9&displaylang=en
  - 5,7 million de PC désinfectés en 15 mois (1 sur 311)
  - Les chevaux de Troie représentent 2/3 des infections
  - 6% des PC infectés par le rootkit Sony
  - 8% des PC infectés par un autre rootkit
  - En mars 2006, 20% des PC désinfectés avaient déjà été infectés
- Les protections de Windows Vista
  - http://blogs.msdn.com/michael_howard/archive/2006/06/12/628207.aspx
- Le jeu des chaises musicales chez Microsoft
  - http://news.com.com/Microsoft+shuffles+more+executives/2100-1022_3-6089338.html?tag=nefd.top
- Le site Cexcellent
  - http://www.microsoft.com/france/technet/cexcellent/

Dernières vulnérabilités
Infos Microsoft (3/3)

EdelWeb

- **Sorties**
  - IE 7 Beta 3
  - Business Desktop Deployment (BDD) 2.5
- **Fin de support Windows XP SP1**
  - 10 octobre 2006
- **Fin de support Windows 98/ME**
  - 11 juillet 2006
  - IDC estime qu'il en reste 70 millions dans le monde …

Dernières vulnérabilités
Autres avis (1/8) – failles

EdelWeb

- 0day Excel (CVE-2006-3059)
  - Affecte : Excel 2000, XP, 2003 et Excel pour Mac
  - Exploit : la faille se situe dans "Excel Repair Mode"
  - Références :
    - http://isc.sans.org/diary.php?storyid=1420
    - http://www.microsoft.com/technet/security/advisory/921365.mspx
  - Virus exploitant cette faille : Mdropper, Booli, Flux
    - S'injecte dans IE pour contourner les FW perso
    - Crée un fichier à la racine de C:\

Dernières vulnérabilités
Autres avis (2/8) – failles

EdelWeb

- **Buffer overflow HLINK.DLL (CVE-2006-3086)**
  - **Affecte :**
    - **Composant "hlink.dll" livré avec Windows**
    - **Exploité via Excel**
  - **Exploit :**
    - **Fichier contenant une URL trop longue**
    - **Il est nécessaire d'ouvrir le fichier puis de cliquer sur l'URL**
  - **Références :**
    - **http://blogs.technet.com/msrc/archive/2006/06/20/437826.aspx**
    - **http://archives.neohapsis.com/archives/fulldisclosure/2006-06/0436.html**
  - **Virus exploitant cette faille : Urxcel.A**

- **Faille Office**
  - **Exécution d'un objet Shockwave Flash sans confirmation de l'utilisateur dans un document Office**
    - **PoC Sous Excel (CVE-2006-3014)**
    - **http://hackingspirits.com/vuln-rnd/vuln-rnd.html**

Dernières vulnérabilités
Autres avis (3/8) – failles

EdelWeb

- Un "bug" dans NOTEPAD (!)
  - Créer un fichier
  - Ecrire "this app can break"
  - Sauvegarder
  - Re-ouvrir le fichier

  - (Bug dû à la détection automatique des caractères Unicode)
  - http://blogs.msdn.com/michkap/archive/2006/06/14/631016.aspx

- Des failles corrigées également dans OpenOffice
  - Exécution de macros sans confirmation
  - Exécution d'applets Java hors du bac à sable
  - "Buffer Overflow" dans le traitement des fichiers XML

- Acheter toutes les failles publiées en 2004 dans le monde coûterait 1% du budget R&D de Microsoft
  - http://www.matasano.com/log/231/vulnerability-research-in-numbers/

Dernières vulnérabilités
Autres avis (4/8) – failles IE

EdelWeb

- 1 vulnérabilité par jour au mois de juillet pour les navigateurs
  - Par HD Moore (Metasploit)
  - http://browserfun.blogspot.com/
- Deux failles publiées dans la nature
  - Abus du .HTA pour inciter un utilisateur à ouvrir un fichier
    - Affecte : IE
  - Lecture de données dans toutes les pages Web ouvertes
    - Affecte : IE + FireFox
    - Exploit : object.documentElement.outerHTML

Dernières vulnérabilités
Autres avis (5/8) – virus

EdelWeb

- McAfee PreScan & BootScan
  - Traite les problématique des rootkits
  - BetaTest en cours
- BitDefender Antirootkit en cours de développement
- Blog McAfee technique
  - http://www.avertlabs.com/research/blog/
- Symantec détecte "Nullsoft Installer" comme un virus
  - Logiciel très populaire (ex. Winamp, Ethereal, …)

Dernières vulnérabilités
Autres avis (6/8) – virus

EdelWeb

- **Initiative CME pas au point ?**
  - **Seulement 8 références en 2006**
  - **http://cme.mitre.org**
- **Yamanner, le premier ver des webmail**
  - **Exploite une faille Yahoo**
- **Faille F-Secure permet de contourner la protection**
  - **http://www.f-secure.com/security/fsc-2006-4.shtml**

Dernières vulnérabilités
Autres avis (7/8)

- **Histogramme des vulnérabilités**
  - Trie par vendeur, produit, version, intervalle de temps, caractéristiques de la vulnérabilité
  - http://nvd.nist.gov/statistics.cfm
- **Outlook supporte nativement jusqu'à 3DES 168 bits**
  - Problème si AES 256 bits est employé pour chiffrer / signer un message
- **experts.microsoft.fr compromis**
  - Certains ont parlé de 0day IIS 6 …
  - Mais la réalité est sans doute beaucoup plus simple ☺

Dernières vulnérabilités
Autres avis (8/8)

EdelWeb

- **DADVSI : le passage en force**
  - **55 amendements ajoutés à la dernière minute**
  - **Les FAI doivent fournir des moyens de filtrage aux abonnés**
  - **Voté le dernier jour de session parlementaire (30 juin)**
  - **http://www.pcinpact.com/actu/news/29601-DADVSI-un-compromis-sans-aucune-opposition.htm?vc=1**
  - **http://www.parti-pirate.info/**

Questions / réponses

EdelWeb

- Questions / réponses
- Date de la prochaine réunion
  - Lundi 11 septembre 2006 ?
- N'hésitez pas à proposer des sujets et des salles
- BONNES VACANCES !