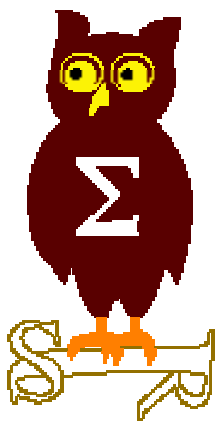
OSSIR
Groupe Sécurité Windows

Réunion du 12 décembre 2005



Revue des dernières vulnérabilités Microsoft

Nicolas RUFF

EADS-CCR

nicolas.ruff@eads.net

Dernières vulnérabilités
Avis Microsoft (1/2)

- (Avis de sécurité Microsoft depuis le 7 novembre 2005)

- Novembre 2005
  - MS05-053 : vulnérabilités multiples dans le rendu EMF/WMF
    - Affecte : Windows 2000 SP4, Windows XP SP1/SP2, Windows 2003 SP0/SP1
    - Exploit : permet d'obtenir les droits SYSTEM (!)
    - Crédit : VenusTech, eEye, Symantec

- Advisories
  - Q910550 : faille exploitable dans Macromedia Flash Player 7
  - Q911052 : fuite mémoire via UPNP (similaire à MS05-047)
  - Q911302 : faille exploitable dans l'appel OnLoad()
    - DoS découvert en mai 2005 et reclassifié en "remote exploit"
    - Exploit : http://www.computerterrorism.com/research/ie/poc.htm
    - Provoque un DoS sur FireFox

Dernières vulnérabilités
Avis Microsoft (2/2)

- **Décembre**
  - 2 bulletins affectant Windows (allant jusqu'à "critique")
  - 2 mises à jour "non sécurité" pour Windows Update (WU) et Software Update Services (SUS)
  - 3 mises à jour "non sécurité" pour Microsoft Update (MU) et Windows Server Update Services (WSUS)

- **Révisions**
  - MS05-050
    - Version 1.4 : interactions avec DirectX
  - MS05-053
    - Version 1.1 : précisions sur la version x64

Dernières vulnérabilités
Infos Microsoft (1/3)

- **Lancement mondial de Visual Studio 2005 et SQL Server 2005**
  - **7 novembre 2005**
  - **2500 personnes sous la pyramide du Louvre**
- **Microsoft s'associe à Cisco pour contrecarrer Skype**
  - **Protocole "ouvert" ICE (Interactive Connectivity Establishment)**
  - **http://www.microsoft.com/presspass/press/2005/nov05/11-09ICENATPR.mspx**
- **Microsoft autorise la vente de licences d'occasion**
  - **Sur le site "discount-licensing.com"**
  - **http://www.zdnet.com.au/news/software/soa/Secondhand_Microsoft_software_goes_on_sale_in_UK/0,2000061733,39221948,00.htm**

Dernières vulnérabilités
Infos Microsoft (2/3)

- **Le noyau "Singularity" se compare à Linux et BSD**
  - **ftp://ftp.research.microsoft.com/pub/tr/TR-2005-135.pdf**
  - **http://blogs.zdnet.com/Murphy/index.php?p=459**
  - **Et Windows XP perd la bataille (en nombre de cycles) !**
    - **Exemple : CreateProcess**
      - **FreeBSD : 1,032,000**
      - **Linux : 719,000**
      - **Windows XP : 5,376,000**

- **Microsoft s'arrange à l'amiable dans un procès antitrust en Corée du Sud**
  - **Indemnité de $30 million versée au portail Daum**
  - **http://www.nytimes.com/2005/11/12/business/worldbusiness/12soft.html?ex=1289451600&en=d74128f10d15aeb3&ei=5088&partner=rssnyt&emc=rss**

- **Microsoft demande l'appui du DOJ dans les procès antitrust européens**
  - **http://www.computerworld.com/governmenttopics/government/story/0,10801,106216,00.html?source=x261**

Dernières vulnérabilités
Infos Microsoft (3/3)

- "Microsoft Research Trustworthy Computing Curriculum 2005 Request for Proposals (RFP)"
  - http://research.microsoft.com/ur/us/fundingopps/RFPs/TWC_Curriculum_2005_RFP.aspx
- Manœuvres autour du format de document "ouvert" dans Office 12
  - http://www.eweek.com/article2/0,1895,1894039,00.asp
- Des mémos internes Microsoft
  - Ray Ozzie (CTO Microsoft)
    - Peu de sécurité et beaucoup de services Web
    - http://www.scripting.com/disruption/ozzie/TheInternetServicesDisruptio.htm
  - Bill Gates : "Microsoft is disrupted"
    - Inquiet du développement de Skype, Google Desktop, Adobe PDF, RIM, SalesForce et iTunes
    - http://www.scripting.com/disruption/mail.html

Dernières vulnérabilités
Autres avis (1/9) - failles

- 2 vulnérabilités RealPlayer
  - Critiques (exploitables via un navigateur)
    - Penser à mettre à jour RealPlayer
  - Crédit : eEye

- Un "0day" en vente sur eBay
  - Rapidement supprimé du site
    - Miroir : http://heapoverflow.com/ebay_joke.htm
  - Microsoft confirme qu'il s'agit bien d'une faille Excel !
    - http://www.eweek.com/article2/0,1759,1899697,00.asp?kc=EWRSS03129TX1K0000614
    - http://nvd.nist.gov/nvd.cfm?cvename=CVE-2005-4131

- Les applications font un usage dangereux de CreateProcess()
  - Exploit : CreateProcess(NULL, "c:\program files\...")
  - Affecte :
    - RealPlayer 10.5, KAV, VMWare Tray, iTunes, Microsoft AntiSpyware Beta
  - Crédit : iDefense

Dernières vulnérabilités
Autres avis (2/9) - failles

- **Faille dans la fonction SynAttackProtect de Windows**
  - Affecte : Windows 2000 tous SP, Windows 2003
    - Corrigé (silencieusement) dans Windows 2000 SP4 URP1, Windows 2003 SP1
  - Exploit :
    - La clé SynAttackProtect permet d'activer les SynCookies
    - Le hash est prédictible, il est donc possible de saturer la table de "lookup"
  - Crédit : Luigi Mori

- **Evasion de la JVM**
  - Affecte : JVM Sun <= 1.4.2_08 et <= 5.0 Update 3
  - Exploit : va probablement être utilisé par des spywares
  - Crédit : Adam Gowdiak (bien connu dans le monde Java)

Dernières vulnérabilités
Autres avis (3/9) – virus et spywares

- **Un blog qui installe des spywares fermé par la FTC**
  - Programme d'affiliation "agressif" de la société Enternet
  - http://www.theregister.com/2005/11/11/spyware_firm_restrained/
- **Trend ne sait plus trop si la faille EMF est exploitée … ou pas**
  - http://news.zdnet.co.uk/0,39020330,39236738,00.htm
- **Mauvais karma pour Kaspersky**
  - http://www.zone-h.org/en/defacements/mirror/id=2987153/
- **Le nombre de Keyloggers explose**
  - +65% de variantes dans la nature l'année dernière
  - 6200 programmes recensés
  - Source : iDefense
  - http://www.zdnet.com.au/news/security/soa/Study_Keystroke_spying_on_the_rise/0,2000061744,39222809,00.htm

Dernières vulnérabilités
Autres avis (4/9) – virus et spywares

- **SpyMon interdit l'analyse du binaire et la détection par les outils de sécurité dans son EULA**
  - **http://www.theregister.co.uk/2005/11/14/spymon/**
- **Les produits antivirus ne scannent pas les fichiers dont le nom comporte des caractères non-MSDOS**
  - **Affecte :**
    - **Kaspersky, Symantec, F-Prot, ClamWin, Avast, RAV, Microsoft AntiSpyware Beta**
  - **Crédit : XFocus**
- **Un "ver" Javascript**
  - **Une attaque simple sur le portail "Myspace" se transforme en DoS de plusieurs heures**
  - **http://www.securityfocus.com/columnists/364**

Dernières vulnérabilités
Autres avis (5/9) – virus et spywares

- **Forte activité du virus Sober**
  - **Adresse source : FBI ou CIA**
  - **Sujet : "Your IP has been logged" ou "You visit illegal websites"**
  - **http://www.washingtonpost.com/wp-dyn/content/article/2005/11/23/AR2005112302147_pf.html**
  - **Hotmail affecté**
    - **http://news.zdnet.co.uk/0,39020330,39240173,00.htm**
- **Un disque USB préinfecté par Backdoor.Win32.Tompai**
  - **http://www.f-secure.com/weblog/#00000723**
- **Quelques vers originaux**
  - **PL/SQL**
    - **http://www.red-database-security.com/advisory/oracle_worm_voyager.html**
  - **PHP (via la faille Mambo) : Linux/Elxbot**
    - **http://www.outpost24.com/**

Dernières vulnérabilités
Autres avis (6/9)

- Une banque suédoise utilisant des OTP victime de phishing
  - http://www.theregister.co.uk/2005/10/12/outlaw_phishing/
- Le président du système Early Warning victime d'une usurpation de CB
  - http://www.theregister.co.uk/2005/05/27/fraud_expert_defrauded/
- Sur le front du P2P
  - La directive EUCD pourrait être adoptée en France le 22 ou 23 décembre (sous le nom de DADVSI)
    - Très restrictif : voir http://www.eucd.info/
  - Dans cette directive, les logiciels P2P doivent intégrer un système de DRM
    - http://www.zdnet.fr/actualites/internet/0,39020774,39286440,00.htm
- Le trésor public migre vers OpenOffice en 2006
  - 80,000 postes
  - http://zdnet.fr/actualites/informatique/0,39040745,39286358,00.htm

Dernières vulnérabilités
Autres avis (7/9)

- **Symantec ne distribue plus L0phtCrack hors US/Canada**
  - **http://www.theregister.co.uk/2005/11/25/symantec_l0phtcrack_export_controversy/print.html**
- **L'Australie met en place un "Early Warning System" contre les botnets avec l'aide des ISP**
  - **http://www.secuobs.com/news/11112005-australie-botnet.shtml**
- **Le cybercrime dépasse le trafic de drogue en volume**
  - **http://smh.com.au/news/technology/cybercrime-now-bigger-than-the-drug-trade/2005/11/29/1133026443366.html**

Dernières vulnérabilités
Autres avis (8/9) – rootkit Sony

- "L'affaire" Sony
  - "La faille était dans le rootkit"
    - http://www.cnn.com/2005/TECH/internet/11/10/sony.hack.reut/index.html
  - "La faille était aussi dans le désintalleur"
    - http://www.freedom-to-tinker.com/?p=927
  - La carte des "utilisateurs" (basée sur les caches DNS)
    - Près de 500,000 *réseaux* "infectés" !
    - http://www.doxpara.com/?q=sony
  - Les créateurs de virus ont vite compris l'intérêt
    - http://www.cnn.com/2005/TECH/internet/11/10/sony.hack.reut/index.html
  - Des violations de GPL / LGPL relevées
    - http://www.the-interweb.com/serendipity/
    - http://hack.fi/~muzzy/sony-drm/

Dernières vulnérabilités
Autres avis (9/9) – rootkit Sony

- Affecte les Mac également ?
  - http://fergdawg.blogspot.com/2005/11/sony-drm-cds-infect-macs-too.html
- Même TF1 en parle !
  - http://news.tf1.fr/news/multimedia/0,,3263001,00.html
- Un EULA restrictif
  - "Les conditions d'usage comprennent l'interdiction d'écouter la musique importée si l'on déménage à l'étranger, ou l'impossibilité d'utiliser la musique pour illustrer un diaporama, même dans le cadre privé."

Questions / réponses

- **Questions / réponses**
- **Date de la prochaine réunion**
  - **Lundi 9 janvier 2006**
  - **AG le 10 janvier**
- **N'hésitez pas à proposer des sujets et des salles**