OSSIR
Groupe Sécurité Windows

Réunion du 10 décembre 2007

Revue des dernières vulnérabilités Microsoft

Cette veille est réalisée par les coanimateurs du groupe Windows

EdelWeb

Olivier REVENU
olivier.revenu (à) edelweb.fr

Mickaël DEWAELE
mickael.dewaele (à) edelweb.fr

Nicolas RUFF
EADS-IW
nicolas.ruff (à) eads.net

Dernières vulnérabilités
Avis Microsoft (1/3)

- **Correctifs de Novembre 2007**
  - **MS07-061 Correctif pour la faille ShellExecute()**
    - **Affecte : Windows XP et 2003**
    - **Exploit :**
      - **Erreur présente dans shell32.dll**
      - **Exploitable facilement via IE7**
    - **Crédit :**
      - **Jesper Johansson, Carsten H. Eiram / Secunia, Aviv Raff / Finjan, Petko Petkov / GNUCITIZEN**
  - **MS07-062 Spoofing DNS**
    - **Affecte : Windows 2000 Server, Windows 2003**
    - **Exploit : spoofing de réponses DNS**
    - **Crédit :**
      - **Alla Berzroutchko / Scanit, Amit Klein / Trusteer**

Dernières vulnérabilités
Avis Microsoft (2/3)

- **Prévisions pour Décembre 2007**
  - 6 bulletins Windows, allant jusqu'à "critique"
  - 1 bulletin Internet Explorer, de niveau "critique"
- **Advisories**
  - Q945713 : utilisation du nom "WPAD" par Internet Explorer

Dernières vulnérabilités
Avis Microsoft (3/3)

- **Révisions**
  - **MS07-049 Faille Virtual PC/Virtual Server**
    - **Version 2.0 : problème d'installation avec la version 1.0**
  - **MS07-061**
    - **Version 1.1 : ce bulletin ne remplace pas MS07-006**

Dernières vulnérabilités
Infos Microsoft (1/4) - sorties

- Sorties logicielles
  - "Viridian" devient "Hyper-V"
  - Microsoft Search Server 2008
  - Visual Studio 2008
  - Windows CE 6 R2
  - Exchange 2007 SP1
  - .NET Framework : 2.0 SP1, 3.0 SP1, 3.5 RTM
  - SQL Server Compact 3.5

- Disponible sur MSDN
  - Windows XP SP3 RC
    - http://4sysops.com/archives/download-windows-xp-sp3-rc1-with-this-little-hack/
  - Vista SP1 RC
    - http://www.ghacks.net/2007/10/14/download-windows-vista-service-pack-1-beta/
  - Windows 2008 RC1

Dernières vulnérabilités
Infos Microsoft (2/4) - sécurité

- Une faille dans CryptGenRandom()
  - Affecte : au moins Windows 2000
  - Exploit : la prédiction de la sortie de CryptGenRandom() pour un processus donné est au maximum en 2^23
  - http://eprint.iacr.org/2007/419.pdf

- A mettre en rapport avec la "backdoor" NSA dans le générateur "Dual_EC_DRBG" ?
  - http://www.schneier.com/blog/archives/2007/11/the_strange_sto.html
  - http://rump2007.cr.yp.to/15-shumow.pdf

- Problème de mise à jour WSUS
  - Un guillemet double dans la description d'un correctif provoque le plantage du serveur
  - http://isc.sans.org/diary.html?storyid=3637
  - Que faut-il en conclure ? ☺

Dernières vulnérabilités
Infos Microsoft (3/4) - sécurité

- Internet Explorer vs. FireFox …
  - http://blogs.technet.com/security/archive/2007/11/30/download-internet-explorer-and-firefox-vulnerability-analysis.aspx

- Tout ça pour ça
  - Historique :
    - La société Eolas avait breveté le concept d'ActiveX
    - Microsoft a perdu son procès
    - Microsoft a finalement acheté le droit d'exploitation du concept
  - Résultat :
    - La gestion des ActiveX dans IE va "bientôt" revenir dans l'état d'avril 2006
  - http://blogs.msdn.com/ie/archive/2007/11/08/ie-automatic-component-activation-changes-to-ie-activex-update.aspx

Dernières vulnérabilités
Infos Microsoft (4/4) - Vista

- Un document Microsoft contenant les améliorations à apporter à Vista publié sur Internet
  - http://www.neowin.net/images/uploaded/1798_early_feedback.png
- WGA se durcit avec Vista SP1
  - Toutes les techniques connues sont bloquées
  - http://www.microsoft.com/presspass/features/2007/dec07/12-03wga.mspx
- Vista pour 5 euros ?
  - Allez sur http://www.windowsanytimeupgrade.com/
  - Cliquez sur "Achetez maintenant"
  - Choisir "Windows Vista Home Premium"
  - Cliquez sur "Choisir Windows Vista Ultimate"
  - "Avez-vous un DVD Windows Anytime Upgrade?" : répondre Non
  - Supprimer "Windows Vista Home Premium à Windows Vista Ultimate"
  - Remplir le formulaire et valider

Dernières vulnérabilités
Autres avis (1/7) – failles

- **Faille QuickTime 7.3**
  - Affecte : QuickTime <= 7.3
  - Exploit : "buffer overflow" dans le traitement d'un flux RTSP
    - http://research.eeye.com/html/alerts/zeroday/20071123.html
    - http://isc.sans.org/diary.html?storyid=3690
    - http://www.symantec.com/enterprise/security_response/weblog/2007/11/0day_exploit_for_apple_quickti.html
  - Exploité "dans la nature"

- **MD5 cassé par une PlayStation3**
  - Des fichiers PDF et EXE valides ont été générés en 2 jours
    - EXE
      - http://www.win.tue.nl/hashclash/SoftIntCodeSign/
    - Résultat des élections au format PDF
      - http://www.win.tue.nl/hashclash/Nostradamus/

Dernières vulnérabilités
Autres avis (2/7) – failles

- **Faille Windows Media Player**
  - **Affecte : Windows Media Player 6.4**
    - **Version par défaut dans Windows 2000**
  - **Exploit : ouverture d'un fichier ".mp4"**
    - **http://www.securityfocus.com/bid/26773**

- **Déni de service via un pointeur NULL dans WIN32K.SYS**
  - **https://www.openrce.org/blog/view/966/Null_pointer_dereference_in_win32k**

Dernières vulnérabilités
Autres avis (3/7) – failles

- Faille dans le driver Winpcap
  - Affecte : Winpcap < 4.0.2
  - Exploit : Elévation locale de privilèges
    - http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=625

- Failles Lotus Notes
  - Affecte : au moins Notes 7.x
  - Exploit : failles multiples dans le traitement des fichiers Lotus-123
    - http://www.coresecurity.com/index.php5?action=item&id=2008

- FireFox 2.0.0.10
  - Corrige des failles de sécurité
- FireFox 2.0.0.11
  - Corrige des problèmes de la version précédente

Dernières vulnérabilités
Autres avis (4/7) – malwares et spam

- Vers de nouveaux comparatifs antivirus ?
  - http://www.01net.com/editorial/365727/vers-un-test-standard-pour-evaluer-les-antivirus/
- Trojan.Advatrix : une charge originale
  - Réactive les vulnérabilités MDAC (BID 17462) et ANI (BID 23194) sans désinstaller les patches Microsoft !
- Le spam de mieux en mieux filtré
  - http://www.wired.com/techbiz/it/news/2007/11/google_spam
- Méfiez vous des antivols …
  - Celui-ci envoie un SMS toutes les 8 secondes !
  - http://www.f-secure.com/weblog/archives/00001328.html
- Des bots sur les sites de rencontre !
  - http://www.news.com/8301-13860_3-9831133-56.html

Dernières vulnérabilités
Autres avis (5/7) – attaques 2.0

- Encore un CD-ROM perdu
  - … contenant l'ensemble des données personnelles des familles anglaises ayant au moins un enfant de moins de 16 ans
    - 25 millions de personnes
  - Le ministre concerné a dû démissionner
  - http://news.sky.com/skynews/article/0,,70131-1293566,00.html
- Une autre "Data Breach" massif chez SalesForce
  - http://www.australianit.news.com.au/story/0,24897,22724319-15306,00.html
- La loi anglaise obligeant à révéler ses clés de chiffrement va être mise en œuvre pour la première fois
  - Dans une affaire de militants pour la cause animale
  - http://news.bbc.co.uk/1/hi/technology/7102180.stm

Dernières vulnérabilités
Autres avis (6/7) – attaques 2.0

- Encore des *defacements* massifs
  - 40,000 sites Web dans lesquels un lien vers "yl18.net/0.js" a été ajouté

- Encore une faille XSS "grave"
  - Affect : FireFox (seulement ?)
  - Exploit :
    - Utilise le handler "jar:"
    - Conséquences graves sur GMail
      - jar:http://groups.google.com/searchhistory/url?url=http://beford.org/stuff/htm.jar!/htm.htm
    - http://www.gnucitizen.org/blog/severe-xss-in-google-and-others-due-to-the-jar-protocol-issues

- La police intervient pour … un vol de meubles virtuels !
  - Sur le site communautaire Habbo

Dernières vulnérabilités
Autres avis (7/7) – just for fun

- **MS Explorer coule !**

Un navire de croisière coule en Antarctique, ses occupants sains

LEMONDE.FR avec AFP | 23.11.07 | 16h29 • Mis à jour le 23.11.07 | 18h17

Le "MS-Explorer" après avoir heurté un iceberg près des îles Shetland, entre l'Argentine et l'Antarctique, vendredi 23 novembre 2007.

Reuters/REUTERS TV

http://www.lemonde.fr/web/article/0,1-0@2-3222,36-981989,0.html?xtor=RSS-3208

Dernières vulnérabilités
Autres infos (1/4) – just for fun

- Une preuve de concept de spyware pour l'iPhone
  - http://www.fastcompany.com/articles/2007/11/hacking-the-iphone.html
- David Litchfield scanne Internet
  - Résultat :
    - 124,000 serveurs Oracle
    - 368,000 serveurs SQL
  - … directement accessibles depuis Internet
  - http://blogs.zdnet.com/security/?p=663
- La BBC explique la sécurité
  - http://news.bbc.co.uk/media/avdb/news/uk/video/132000/bb/132146_16x9_bb.asx?ad=1&ct=50
  - Dommage qu'ils utilisent MS04-011 en 2007 ☺
- Le social engineering, ça marche toujours
  - "Bonjour, donnez moi votre schéma d'architecture"
  - http://isc.sans.org/diary.html?storyid=3675

Dernières vulnérabilités
Autres infos (2/4) – just for fun

- Une version de FireFox dédiée au Web 2.0 : Flock 1.0
  - http://www.clubic.com/actualite-84924-flock-navigateur-web-social-finalise.html
- Une version de FireFox dédiée … au piratage de Meetic
  - http://www.zataz.com/news/15712/Firefox-Meetic-Edition-pas-payer-service.html
- La plateforme .NET suscite l'intérêt …
  - Compilateur BrainFuck -> .NET
    - http://www.soulsphere.org/stuffage/bf.net/
  - Compilateur LOLCode -> .NET
    - http://blog.notdot.net/archives/32-LOLCode.net-Now-your-LOLCats-can-use-the-CLR!.html
  - Le langage de script Second Life va passer sur .NET également

Dernières vulnérabilités
Autres infos (3/4) – actualité

- La revente de 3Com à Huawei ne fait pas plaisir à tout le monde …
  - http://blogs.zdnet.com/security/?p=705

- Remise du rapport "Olivennes" sur le P2P
  - Largement commenté dans la presse

Dernières vulnérabilités
Autres infos (4/4)

- Et pendant ce temps là sur la mailing liste de l'OSSIR
  - Obligations légales vis-à-vis des journaux
  - Bannière SSH
  - Analyse de fichiers "core"
  - Interdire les logiciels d'accès distant
  - Reverse proxy
  - Certification HON@CODE
- L'appel à communications pour la JSSI 2008 est ouvert !
  - http://www.ossir.org/jssi2008/
  - Thème : "anonymat, vie privée et gestion d'identité"

Questions / réponses

- Questions / réponses
- Date de la prochaine réunion
  - Prochaine réunion le 7 janvier 2008
  - AG le 8 janvier 2008
- N'hésitez pas à proposer des sujets et des salles