OSSIR
Groupe Paris

Réunion du 9 juin 2009

Revue des dernières vulnérabilités

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

Avis Microsoft (1/5)

- **Correctif de Mai 2009**
  - **Avec [*exploitability index*]**
  - **MS09-017 Failles PowerPoint [1,2,1,1,2,2,1,1,1,1,1,1,1,1]**
    - **Affecte: PowerPoint (toutes versions supportées)**
      - **Note: pas de correctif pour PowerPoint sur Mac OS X et Microsoft Works (!)**
    - **Exploit:**
      - **14 failles corrigées**
      - **L'une des deux failles est exploitée dans la nature en "0day"**
    - **Notes:**
      - **http://blogs.technet.com/srd/archive/2009/05/12/ms09-017-an-out-of-the-ordinary-powerpoint-security-update.aspx**
      - **Le support PowerPoint 4.0 est maintenant désactivé par défaut**
      - **Une partie du moteur a été réécrite**

Avis Microsoft (2/5)

- Crédit:
  - iDefense (x10)
    - anonymous (x2)
    - Sean Larsson (x3)
    - Marsu Pilami (x5)
    - http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=787
    - (...)
    - http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=796
  - ZDI (x2)
    - Marsu Pilami
    - Ling and Wushi / team509
    - http://www.zerodayinitiative.com/advisories/ZDI-09-019/
    - http://www.zerodayinitiative.com/advisories/ZDI-09-020/
  - Secunia
    - Carsten H. Eiram
    - http://secunia.com/secunia_research/2008-46/
  - VUPEN
    - Nicolas Joly (x2)

Avis Microsoft (3/5)

- A noter également
  - Mises à jour WSUS
    - http://support.microsoft.com/kb/894199
  - Mises à jour "non sécurité"
    - http://technet.microsoft.com/en-us/wsus/bb466214.aspx

Avis Microsoft (4/5)

- Advisories
  - 969136
    - Corrigé par MS09-017
  - 971492
    - Faille "0day" dans le support WebDAV sur IIS <= 6.0
  - 971778
    - Faille "0day" dans DirectX 7.0 – 9.0 (support QuickTime)
      - http://blogs.technet.com/srd/archive/2009/05/28/new-vulnerability-in-quicktime-parsing.aspx
- Prévisions pour Juin 2009
  - Windows: critique (x2), important (x3), modéré (x1)
  - IE: critique (x1)
  - Word: critique (x2)
  - Excel: critique (x1)

Avis Microsoft (5/5)

- Révisions
  - MS07-026
    - Version 1.1: changement dans la logique de détection
  - MS09-003
    - Version 3.0: changement dans la logique de détection sur Exchange 2003 SP2
  - MS09-008
    - Version 2.0: distribution du patch MS08-066 pour les machines qui ne font pas office de serveur DNS
  - MS09-017
    - Version 1.1: mise à jour de la documentation

Infos Microsoft (1/2)

- **Sorties logicielles**
  - **Un plugin "SDL" pour Visual Studio**
    - **http://msdn.microsoft.com/fr-fr/security/dd670265(en-us).aspx**
  - **Microsoft Axum**
    - **Un environnement pour le massivement parallèle en .NET**
  - **Beta(s)**
    - **Visual 2010 et .NET Framework 4.0 Beta1**
  - **Windows Seven pour le 22 octobre**
    - **RTM fin juillet**

Infos Microsoft (2/2)

- **Autre**
  - "Live" devient "Bing"
  - memcpy() devient une API "officiellement dangereuse"
    - http://blogs.msdn.com/sdl/archive/2009/05/14/please-join-me-in-welcoming-memcpy-to-the-sdl-rogues-gallery.aspx
  - Le format "base de registre" entièrement documenté
    - http://amnesia.gtisc.gatech.edu/~moyix/suzibandit.ltd.uk/MSc/
  - Office 2010 supportera des fonctions de mise en page avancées
    - Un futur concurrent à TeX ?
    - http://tech.slashdot.org/article.pl?sid=09/05/19/1556203

Infos Microsoft (2/2)

- IE8 + Windows Live = fail
  - http://support.microsoft.com/kb/970306
- L'installation silencieuse du plugin ClickOnce dans FireFox fait grincer des dents
  - http://voices.washingtonpost.com/securityfix/2009/05/microsoft_update_quietly_insta.html

Infos Réseau

- Déni de service (?) dans les IPSec Tools
  - Affecte: IPSec < 0.7.2
  - Exploit:
    - http://www.certa.ssi.gouv.fr/site/CERTA-2009-AVI-190/CERTA-2009-AVI-190.html

- Faille "TFTP" dans de nombreux produits Cisco
  - Affecte: nombreux logiciels Cisco sous Windows
    - Tous basés sur CiscoWorks Common Services 3.x
  - Exploit: utilisation de la séquence "..\" sous Windows (!)
    - http://www.cisco.com/warp/public/707/cisco-sa-20090520-cw.shtml
    - http://www.cisco.com/warp/public/707/cisco-amb-20090520-cw.shtml

Infos Unix

- **Failles**
  - **Faille(s) dans le noyau dans Linux**
    - **Affecte: Linux < 2.6.29.3**
    - **Exploit:**
      - **http://www.kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.29.3**
      - **Elévation de privilèges via ptrace_attach()**
        - **http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1527**
      - **Fuite d'information via /proc permettant de contourner ASLR**
        - **http://www.cr0.org/paper/to-jt-linux-alsr-leak.pdf**
        - **http://code.google.com/p/fuzzyaslr/**
      - **Et d'autres ... ?**
  - **OpenSSL**
    - **Affecte: 0.9.8k et antérieures**
    - **Exploit: fuites mémoire dans le support DTLS**
  - **Autres ...**
    - **ntpd < 4.2.4p7, Cyrus SASL < 2.1.22, ...**

Infos Unix

- Failles dans sadmind (x2)
  - Affecte: Solaris 8 et 9
  - Exploit: exécution de code à distance via le démon sadmind
    - http://sunsolve.sun.com/search/document.do?assetkey=1-66-259468-1

Infos Unix

- Autre
  - Toutes les clés DSA générées par GnuTLS sont corrompues
    - http://article.gmane.org/gmane.comp.encryption.gpg.gnutls.devel/3516
  - Debian forke Glibc (...)
    - Projet Eglibc
      - http://developers.slashdot.org/article.pl?sid=09/05/06/2050216
    - Suite à:
      - http://sourceware.org/bugzilla/show_bug.cgi?id=5070#c5

Failles

- **Principales applications**

  - **Adobe Acrobat**
    - **Affecte: Acrobat Reader < 8.1.5, < 9.1.1**
      - **Et probablement toutes les versions antérieures ...**
      - **Fonctions JavaScript getAnnots() & spell.customDictionaryOpen()**
    - **Exploit:**
      - **http://www.adobe.com/support/security/advisories/apsa09-02.html**
      - **http://www.adobe.com/support/security/bulletins/apsb09-06.html**
    - **Notes:**
      - **Pas (encore) de correctif pour les utilisateurs d'Acrobat 7.1.2 sur Mac OS X**
    - **Promis, Adobe va faire mieux ...**
      - **http://blogs.adobe.com/asset/2009/05/adobe_reader_and_acrobat_secur.html**

Failles

- Mac OS X
  - Affecte: Mac OS X < 10.5.7
  - Exploit:
    - 67 failles corrigées ...
    - http://dvlabs.tippingpoint.com/advisory/TPTI-09-04
  - Notes:
    - Incompatible avec l'antivirus Sophos
      - http://www.sophos.com/support/knowledgebase/article/58562.html
    - Heureusement qu'il n'y a pas besoin d'antivirus sur Mac OS X ☺

- Une faille Java toujours présente dans Mac OS X
  - Connue et documentée depuis 1 an ...
    - http://blog.cr0.org/2009/05/write-once-own-everyone.html
  - A voir aussi ...
    - http://slightlyrandombrokenthoughts.blogspot.com/2009/04/timeline-of-sun-microsystems-fixing.html
    - http://voices.washingtonpost.com/securityfix/applejava.htm

Failles

- QuickTime (n'en jetez plus !)
  - Affecte:
    - iTunes < 8.2
    - QuickTime < 7.6.2
  - Exploit: multiples
    - ... dont le fabuleux "itms://A*1000" dans iTunes
      - http://dvlabs.tippingpoint.com/advisory/TPTI-09-03

Failles

- *BlackBerry Attachment Service*
  - Affecte: BES 4.1.x et 5.0.x
  - Exploit: exécution de code lors de la conversion d'un document PDF
    - http://www.blackberry.com/btsc/search.do?cmd=displayKC&docType=kc&externalId=KB18327
  - Dommage car le BES 5.0 vient d'être certifié EAL4+ ...
    - http://www.globalsecuritymag.fr/BlackBerry-Enterprise-Server,20090505,8980
- Egalement ...
  - WireShark < 1.0.8
  - Xerox WorkCenter
    - http://www.xerox.com/downloads/usa/en/c/cert_XRX09-02_v1.0.pdf

Malwares et spam

- McAfee rachète SolidCore
  - Le "white listing" devient tendance
    - http://www.solidcore.com/
- Que signifient "PCI" et "McAfee Secure" ?
    - http://skeptikal.org/2009/05/epic-failure-from-mcafee.html
- Communication McAfee
    - http://www.stophcommerce.com/
- Un antivirus en Klingon ...
  - Qui a dit que le marché de l'antivirus n'était que du marketing ?
    - http://www.sophos.com/klingon-anti-virus/

Failles 2.0

- Un bon exemple d'effet boule de neige
  - DDoS sur un DNS
  - + problème dans la logique de mise à jour de Baofeng
  - = DDoS sur China Telecom

- Facebook adopte OpenID
  - http://www.lemondeinformatique.fr/actualites/lire-facebook-adopte-le-standard-d-authentification-open-id-28617.html

- Toutes les données techniques et commerciales de T-Mobile à vendre
  - http://archives.neohapsis.com/archives/fulldisclosure/2009-06/0063.html

- Astalavista.com FAIL
  - http://seclists.org/fulldisclosure/2009/Jun/0048.html

Failles 2.0

- L'écoute de SMS avec un Nokia 1100 ne serait pas un *fake*
  - http://www.networkworld.com/news/2009/052109-investigators-replicate-nokia-1100-online.html
- Challenge de sécurité FAIL
  - Au départ: $10,000 pour rentrer dans une adresse email
    - http://www.strongwebmail.com/news/secure-web-mail/break-into-my-email-get-10000-here-is-my-username-and-password/
  - Au final: XSS ...
    - http://twitpic.com/6ji72/full
    - http://blogs.zdnet.com/security/?p=3514

Actualité (France)

- **LOPPSI 2 : vous n'avez encore rien vu**
  - **http://www.lemonde.fr/technologies/article/2009/05/18/apres-la-dadvsi-et-hadopi-bientot-la-loppsi-2_1187141_651865.html**
- **245,000 mots de passe Orange dans la nature**
  - **Suite à une injection SQL triviale**
    - **http://technicalinfodotnet.blogspot.com/2009/05/orangefr-sql-injection-245000-clear.html**
- **InfoSecurity 2009 annulé**
- **Free active le "FreeWifi"**

Actualité (anglo-saxonne)

- Le gouvernement anglais veut surveiller tout le trafic IP
  - (Internet et VoIP)
    - http://www.timesonline.co.uk/tol/news/politics/article6211101.ece
- La dépendance aux infrastructures critiques ... pour de vrai
    - http://libertesinternets.wordpress.com/2009/04/26/il-suffit-dun-secateur-pour-paralyser-une-ville-de-50-000-habitants/
- Renforcement de la sécurité informatique
  - ... dans le domaine de l'énergie
    - http://www.csoonline.com/article/491943/New_Cyber_Security_Standards_for_N._American_Power_System
- Obama met le paquet sur la cybersécurité
    - http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/

Actualité (anglo-saxonne)

- Jeff Moss appointé au *Homeland Security Advisory Council*
  - *http://news.cnet.com/8301-1009_3-10258634-83.html*
- Des serveurs militaires américains piratés par des turcs
  - Groupe "m0sted"
    - http://www.informationweek.com/news/showArticle.jhtml?articleID=217700619
- Le DoD ouvre sa propre "forge"
  - Notez le certificat SSL non trusté ☺
    - https://www.forge.mil/
- DMCA vs. parodies de "La Chute"
  - http://ideas.4brad.com/hitler-tries-dmca-takedown
  - Un lecteur de flux RSS connecté à l'EFF a été retiré de l'AppStore (!)
    - http://ideas.4brad.com/apple-blocks-iphone-app-because-eff-blog-points-my-downfall-parody

Actualité (Google)

- Un premier pas vers le SLA pour les applications Google
  - http://www.google.com/appsstatus#
- Google ajoute le chat vidéo à GMail/GTalk
  - http://mail.google.com/videochat

Actualité

- Intel condamné à plus d'un milliard de dollars d'amende
  - Par la commission européenne, pour abus de position dominante
    - http://www.lesechos.fr/info/hightec/4864191-bruxelles-inflige-a-intel-une-amende-record.htm
  - A voir aussi:
    - http://www.dailycupoftech.com/2009/05/08/rock-star-geeks/
- Les coûts directs et indirects du vol de *laptop*
  - Attention, étude sponsorisée ...
    - http://communities.intel.com/docs/DOC-3076
- Le coût de correction des failles Web
  - Environ $28,000 par application (à la louche !)
    - http://jeremiahgrossman.blogspot.com/2009/05/mythbusting-secure-code-is-less.html

Actualité

- 100,000 sites Web effacés en une attaque
  - En cause: le produit de virtualisation applicative HyperVM
    - http://www.theregister.co.uk/2009/06/08/webhost_attack/
  - L'auteur du logiciel se suicide
    - http://www.channelregister.co.uk/2009/06/09/lxlabs_funder_death/
- Le problème des taux de transfert résolu
  - Amazon prend les disques USB pour les envoyer dans le Cloud
    - http://aws.amazon.com/importexport/
- Le site Avsim entièrement perdu suite à une intrusion
    - http://news.bbc.co.uk/2/hi/technology/8049780.stm
- Wojciech Purczynski (alias cliph @ isec.pl) meurt dans un accident d'avion

Actualité

- L0phtCrack, le retour
  - En version 6
    - http://www.l0phtcrack.com/
- Apple recrute Ivan Krstić
  - Ex. participant au projet OLPC
    - http://www.mac4ever.com/news/44534/apple_travaille_avec_un_genie_de_la_securite_informatique/
- La Chine "développe" son propre OS sécurisé: Kylin
    - http://kylin.org.cn/
  - En fait FreeBSD 5.3 (!)
    - http://blogs.zdnet.com/security/?p=3385
- FreeRunner / OpenMoko ... c'est fini !
    - http://mobile.slashdot.org/article.pl?sid=09/04/04/228240

Fun

- RayTracing ... en JavaScript
  - http://jupiter909.com/mark/jsrt.html
- Impossible de regarder un DVD à bord de la navette Atlantis
  - ... pour cause de DRM ? ☺
    - http://apnews.myway.com//article/20090522/D98BF91G0.html

Questions / réponses

- Questions / réponses
- Prochaine réunion
  - Mardi 7 juillet 2009
- N'hésitez pas à proposer des sujets et des salles