OSSIR
Groupe Paris

Réunion du 8 décembre 2009

Revue des dernières vulnérabilités

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

Avis Microsoft (1/9)

- **Correctif de Novembre 2009**
  - **6 bulletins, 15 failles**
  - **Avec [exploitability index]**
  - **MS09-063 Faille dans WSDAPI [2]**
    - **Affecte: Windows Vista & 2008**
      - **WSDAPI = *Web Services on Devices API***
      - **En écoute sur les ports TCP/5357, TCP/5358**
      - **Broadcast UDP/3702 pour la découverte de services**
      - **http://blogs.technet.com/srd/archive/2009/11/10/vulnerability-in-web-services-on-devices-wsd-api.aspx**
    - **Exploit: exécution de code à distance (corruption mémoire)**
    - **Crédit: Neel Mehta / Google**

Avis Microsoft (2/9)

- **MS09-064 Faille dans LLS (*License Logging Server*) [2]**
  - **Affecte: Windows 2000**
  - **Exploit: exécution de code à distance (*heap overflow*)**
    - **LLS est un service RPC accessible anonymement**
    - **http://dvlabs.tippingpoint.com/advisory/TPTI-09-07**
    - **http://blogs.technet.com/srd/archive/2009/11/10/details-on-the-license-logging-service-vulnerability.aspx**
  - **Crédit: Cody Pierce / TippingPoint**

Avis Microsoft (3/9)

- MS09-065 Failles noyau (x3) [2,1,1]
  - Affecte: Windows (toutes versions supportées, sauf Seven et 2008 R2)
  - Exploit: élévation de privilèges locale
    - Déréférencement d'un pointeur NULL dans win32k.sys
    - Problème de traitement d'un paramètre dans win32k.sys
    - Problème dans le support des fichiers EOT dans win32k.sys (exploitable à distance via Internet Explorer)
    - http://blogs.technet.com/srd/archive/2009/11/10/font-directory-entry-parsing-vulnerability-in-win32k-sys.aspx
  - Crédit:
    - Agin Sun
    - Tavis Ormandy / Google (faille EOT)

Avis Microsoft (4/9)

- MS09-066 Déni de service sur Active Directory [3]
  - Affecte: toutes versions de Windows supportant AD ou ADAM
    - (sauf Window Seven et 2008 R2)
  - Exploit: requête récursive infinie
    - exploitable via TCP/389 (LDAP), TCP/636 (LDAP + SSL), TCP/3268 (Global Catalog), TCP/3269 (Global Catalog + SSL)
  - Crédit: n/d

Avis Microsoft (5/9)

- MS09-067 Failles Excel (x8) [2,2,1,1,1,2,2,2]
  - Affecte: Excel, Excel Viewer, Excel pour Mac
    - Non affecté: Works, SharePoint
  - Exploit: exécution de code à l'ouverture d'un document malformé
    - http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=832
    - http://www.zerodayinitiative.com/advisories/ZDI-09-082/
    - http://www.zerodayinitiative.com/advisories/ZDI-09-083/
  - Crédit:
    - Bing Liu / Fortinet (x3)
    - Nicolas Joly / VUPEN (x4)
    - ZDI (x2)
    - Sean Larsson / iDefense (x1)

Avis Microsoft (6/9)

- MS09-068 Faille Word [1]
  - Affecte: Office (toutes versions supportées, sauf Office 2007 et Works)
  - Exploit: exécution de code à l'ouverture d'un document malformé
    - http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=831
  - Crédit: Jun Mao / iDefense

Avis Microsoft (7/9)

- **Prévisions pour Décembre 2009**
  - **6 bulletins, 12 failles**
  - **Sont concernés: Windows, Internet Explorer, Project**
  - **La faille IE6/IE7 exploitée actuellement en "0day" sera corrigée**
  - **Un exploit est disponible dans Metasploit depuis le 25/11/2009**

Avis Microsoft (8/9)

- Advisories
  - 977544: Déni de service sur Windows Seven / 2008 R2
    - Exploitable via un paquet SMBv1 ou SMBv2
      - http://www.microsoft.com/technet/security/advisory/977544.mspx
  - 977981: Faille dans IE6 / IE 7
    - La faille se trouve dans getElementsByTagName()
    - Exploitable classiquement
      - http://blogs.technet.com/msrc/archive/2009/11/23/microsoft-security-advisory-977981-released.aspx

Avis Microsoft (9/9)

- Révisions

  - MS08-076
    - V5.0: Windows Embedded est vulnérable
  - MS09-045
    - V2.0: JScript 5.7 sur Windows 2000 SP4 est affecté
  - MS09-046
    - V1.2: ajout d'un problème connu
  - MS09-051
    - V2.0: problème de détection de la faille sur Windows 2000 SP4
  - MS09-065
    - V1.1: ajout d'un problème connu

Infos Microsoft

- **Sorties logicielles**
  - **3 nouveaux outils de sécurité Web en CTP**
    - **CAT.NET 2.0**
    - **WACA 1.0 (Web Application Configuration Analyzer)**
    - **WPL 1.0 (Web Protection Library)**
    - **http://blogs.msdn.com/securitytools/archive/2009/11/11/some-new-software-security-tools-for-web-developers-ctp-releases.aspx**
  - **Virtual Server 2005 R2 SP1**

Infos Microsoft

- **Autre**
  - **Lancement officiel de la solution Azure au 1er janvier 2010**
    - **http://www.itespresso.fr/microsoft-propulsera-windows-azure-dans-les-nuages-le-1er-janvier-2010-32442.html**
  - **Modification des moteurs antivirus dans ForeFront**
    - **AhnLab, CA et Sophos ne sont plus supportés au 1er décembre 2009**
      - **http://blogs.technet.com/fss/archive/2009/10/21/action-required-by-dec-1-2009-keep-your-protection-current.aspx**
  - **Microsoft brevète la commande "sudo"**
    - **... ou plutôt le fait de présenter une boite de dialogue avec la liste des comptes utilisateurs**
      - **http://gizmodo.com/5402796/microsoft-patents-the-sudo-command**
  - **Un honeypot FTP permet de voir quels sont les mots de passe les plus "scannés"**
    - **L'utilisateur "administrateur" arrive deuxième !**
      - **http://blogs.technet.com/mmpc/archive/2009/11/27/do-and-don-ts-for-p-w0rd.aspx**

Infos Microsoft

- La NSA a participé à la conception de Windows Seven
  - Comme toutes les versions antérieures de Windows
    - http://www.computerworld.com/s/article/9141182/Microsoft_denies_it_built_backdoor_in_Windows_7
- Communication FAIL ?
    - http://www.neverafk.fr/
- Microsoft humilié
  - Confusion entre memcpy(dst, src, size) et memcpy(dst, size, src)
  - ... dans tous les composants d'intégration Hyper-V pour Linux
    - http://patchwork.kernel.org/patch/59443/
- Un outil de déchiffrement BitLocker
  - Sous réserve d'avoir récupéré les clés en mémoire
    - http://arstechnica.com/microsoft/news/2009/12/first-commercial-tool-cracks-bitlocker.ars

Infos Réseau

- **Principales failles**
  - **Faille dans la renégociation TLS**
    - **OpenSSL patché (0.9.8l)**
    - **OpenVPN non vulnérable mais patché (2.1_rc21)**
      - **http://article.gmane.org/gmane.network.openvpn.devel/2835**
    - **MatrixSSL patché (1.8.8)**
      - **http://www.matrixssl.org/archives/cat_releases.html**
    - **Citrix vulnérable**
      - **http://support.citrix.com/article/CTX123359**
    - **Cisco en cours d'investigation ...**
    - **Quelques explications**
      - **http://www.securegoose.org/2009/11/tls-renegotiation-vulnerability-cve.html**
    - **La faille est (était) exploitable contre Twitter pour extraire les logins / mots de passe**
      - **http://www.theregister.co.uk/2009/11/14/ssl_renegotiation_bug_exploited/**

Infos Réseau

- Les VPN SSL, sources de failles Web
  - http://www.kb.cert.org/vuls/id/261869
- Faille dans BIND (corruption de cache)
  - Seulement lorsque DNSSEC est utilisé ...
    - https://www.isc.org/node/504

Infos Unix

- (Principales) failles
  - Wordpress < 2.8.6
    - http://wordpress.org/development/2009/11/wordpress-2-8-6-security-release/
  - PHP < 5.3.1
    - Plus de 100 bogues corrigés
      - http://www.php.net/ChangeLog-5.php#5.3.1
    - Dont un DoS dans le traitement des requêtes POST "multipart/form-data"
      - http://www.john-jean.com/blog/securite-informatique/denial-of-service-php-sur-toutes-les-versions-inferieures-a-5-3-1-301
  - Samba 3.x
    - Faille locale dans mount.cifs (setuid)
      - http://www.samba.org/samba/security/CVE-2009-2948.html
    - DoS distant (après authentification)
      - http://www.samba.org/samba/security/CVE-2009-2906.html
    - Absence de "homedir" pour un utilisateur => partage de "/"
      - http://www.samba.org/samba/security/CVE-2009-2813.html

Infos Unix

- MySQL < 5.0.88, < 5.1.41
  - Problème dans la gestion des certificats
    - Si depth > verify_depth, le certificat est toujours valide (!)
  - Dénis de service à distance
  - Et autres corrections
    - http://dev.mysql.com/doc/refman/5.0/en/news-5-0-88.html
    - http://dev.mysql.com/doc/refman/5.1/en/news-5-1-41.html

- FreeBSD
  - Affecte: 7.1 et 8.0 (au moins)
  - Exploit:
    - Elévation de privilèges locale (toutes versions)
    - Via fichier suid + variables d'environnement ...
      - http://seclists.org/fulldisclosure/2009/Nov/371

- Evasion de QEmu
  - A cause d'une faille dans VNC
    - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3616

Infos Unix

- Audit de code vs. application PHP
  - 40 failles trouvées d'un seul coup dans Simple Machine Forum
    - http://seclists.org/fulldisclosure/2009/Dec/24

- Backdoor dans le serveur HPOV Operations Manager
  - Un compte "en dur" dispose d'un accès irrévocable au répertoire "/manager/html/upload"
    - http://www.zerodayinitiative.com/advisories/ZDI-09-085/

Infos Unix

- **Autre**
  - **Sortie de FreeBSD 8.0**
    - **http://www.freebsd.org/releases/8.0R/pressrelease.html**
  - **Les utilisateurs locaux (console) autorisés à installer des applications sous Fedora 12 ?**
    - **Un bon troll en tout cas**
      - **https://www.redhat.com/archives/fedora-devel-list/2009-November/msg00945.html**
      - **http://lwn.net/Articles/362708/**

Failles

- **Principales applications**
  - **Mac OS X 10.6.2 (applicable à 10.5.8 également)**
    - **Corrige plusieurs dizaines de failles**
      - **http://support.apple.com/kb/HT3937**
    - **Note: Mac OS X 10.4 n'est plus supporté**
  - **Java < 1.5.0_22, < 1.6.0_17 (et versions antérieures)**
    - **Windows, Linux**
      - **http://sunsolve.sun.com/search/document.do?assetkey=1-66-270474-1**
    - **Mac OS**
      - **APPLE-SA-2009-12-03-1, APPLE-SA-2009-12-03-2**
      - **http://support.apple.com/kb/HT3969**
      - **http://support.apple.com/kb/HT3970**
  - **Opera < 10.10**
      - **http://www.opera.com/support/kb/view/941/**
      - **http://www.opera.com/support/kb/view/942/**

Failles

- Safari < 4.0.4
  - http://support.apple.com/kb/HT3949
- Google Chrome < 3.0.195.33
  - http://googlechromereleases.blogspot.com/2009/11/stable-update-fix-google-chrome-not.html

Failles

- Flash Player 10
  - Un patch "critique" publié le 8 décembre pour corriger une faille exploitée dans la nature
    - http://www.adobe.com/support/security/bulletins/apsb09-19.html
    - http://blogs.adobe.com/psirt/2009/12/pre-notification_-_security_up.html
- Faille dans le convertisseur PDF sur le BES
  - Pas de correctif disponible à la date de publication
    - http://www.blackberry.com/btsc/search.do?cmd=displayKC&docType=kc&externalId=KB19860
- VMWare ESX 4.0
  - Uniquement des librairies tierce partie
    - http://lists.vmware.com/pipermail/security-announce/2009/000070.html
- MuPDF / SumatraPDF
  - Pourtant considéré comme "plus sûr" car ne supportant pas JavaScript
    - http://archives.neohapsis.com/archives/fulldisclosure/2009-11/0330.html

Failles 2.0

- Contournement de la Same Origin Policy avec Flash
  - http://www.foregroundsecurity.com/flash-origin-policy-issues.html
- Facebook attaqué
  - Accès à des données de profil non publiques
    - http://www.zataz.com/news/19635/facebook-fuite-de-donnees.html
    - Note: il y en a eu d'autres
  - Démonstration de la prise de contrôle de groupes
    - http://controlyour.info/blog/

Malwares et spam

- Deux utilisateurs du malware Zeus arrêtés à Manchester
  - http://www.pcworld.com/article/182487/uk_police_reveal_arrests_over_zeus_banking_malware.html
- Le manuel du parfait spammer publié en ligne
  - Par erreur ?
    - http://www.net-security.org/secworld.php?id=8453
- 4 ans de prison pour la manipulation de cours en ligne
  - http://www.zdnet.fr/actualites/internet/0,39020774,39711010,00.htm
- Symantec victime d'une injection SQL majeure
  - http://unu123456.baywords.com/2009/11/23/symantec-exposed-passwordsserials-sql-injection-full-database-access/

Actualité (France)

- Ouverture d'un OzSSI à Paris
  - http://www.ssi.gouv.fr/ozssi
- Le "droit à l'oubli numérique" débattu à l'ONU
  - http://www.itespresso.fr/droit-a-l-oubli-sur-internet-nkm-veut-ouvrir-le-debat-au-niveau-de-l-onu-32362.html
- La notification en cas de perte de données
  - ... obligatoire (au moins pour les FAI) en Europe ?
    - http://www.out-law.com/page-10497
- Le nom de domaine "jaimelesartistes.fr" a expiré
  - Il a été promptement récupéré par les anti-HADOPI
    - http://eco.rue89.com/2009/11/09/oups-le-site-officiel-pro-hadopi-change-de-camp-125255

Actualité (France)

- Gandi passe la 6ème
  - http://iwi.lebardegandi.net/post/2009/11/09/Votre-serveur-en-IPV6
- Le décret d'officialisation du RGI publié au journal officiel
  - Il y aura donc 2 formats "officiels" pour les documents XML (OpenOffice et Office 2007)
- Une jurisprudence intéressante
  - Le fondateur de VUPEN condamné à 1000€ d'amende pour "mise à disposition d'outils manifestement (...)"
- HADOPI 2 sera-t-il applicable ?
  - Il fallait peut-être se poser la question avant de voter
    - http://www.pcinpact.com/actu/news/54271-franois-loos-vote-hadopi-securisation.htm

Actualité (anglo-saxonne)

- La surveillance globale d'Internet s'organise aussi en Angleterre
  - http://news.bbc.co.uk/2/hi/uk_news/politics/8350660.stm
  - ... mais la riposte graduée fait débat
    - http://www.timesonline.co.uk/tol/news/uk/crime/article6885923.ece
- Les anglais simulent une panne totale de téléphonie
  - http://www.computing.co.uk/computing/news/2252600/government-simulate-total
- Les américains et la cyberguerre
  - http://www.cbsnews.com/stories/2009/11/06/60minutes/main5555565.shtml?tag=col1;post-4865
  - ... sauf que les pannes électriques ne sont *pas* dues aux hackers
    - http://erratasec.blogspot.com/2009/11/brazil-outage-not-caused-by-hackers.html
- Le directeur du FBI a (presque) été victime de *phishing*
  - Sa femme lui interdit désormais d'utiliser son PC
    - http://news.cnet.com/8301-27080_3-10370164-245.html

Actualité (anglo-saxonne)

- Etre innocent ... et ne pas être assez riche pour pouvoir le prouver
  - http://www.numerama.com/magazine/14449-des-internautes-accuses-a-tort-de-pedophilie.html
  - http://www.lefigaro.fr/web/2009/11/10/01022-20091110ARTFIG00680-ce-virus-qui-telecharge-des-images-pedophiles-.php
- Les FAI américains bientôt responsables des contenus transportés ?
  - http://blogs.pcmag.com/securitywatch/2009/11/proposed_bill_would_make_isps.php
- De nouvelles certifications à gogo
  - Par exemple "Certified Secure Software Lifecycle Professional"
    - http://www.isc2.org/csslp-certification.aspx
- L'armée américaine achète 2200 PS3 supplémentaires
  - http://www.informationweek.com/news/software/linux/showArticle.jhtml?articleID=221900487

Actualité (anglo-saxonne)

- Le FBI a demandé plus de 8 millions de localisations GPS chez l'opérateur Sprint l'année dernière
  - http://www.wired.com/threatlevel/2009/12/gps-data/
- Les fournisseurs de services ne souhaitent pas communiquer sur le prix d'une écoute numérique
  - http://rawstory.com/2009/12/yahoo-spying-policy-shock-customers/

Actualité (Google)

- Chrome OS: ça se précise
  - Version courte:
    - http://www.korben.info/chrome-os-sortie.html
  - Version longue:
    - http://www.chromium.org/chromium-os/chromiumos-design-docs/security-overview
    - http://sites.google.com/a/chromium.org/dev/chromium-os/chromiumos-design-docs/system-hardening
    - http://blog.chromium.org/2009/11/hello-open-source-developers-would-you.html
    - (...)
- Microsoft trouve une faille (un XSS) dans Chrome Frame
  - C'est la guerre ☺
    - http://blogs.zdnet.com/security/?p=4962

Actualité (Google)

- Google DNS
  - http://code.google.com/speed/public-dns/docs/intro.html
- Google SPDY pour remplacer HTTP
  - http://sites.google.com/a/chromium.org/dev/spdy/spdy-whitepaper
- Google GO pour remplacer Python et C/C++
  - http://golang.org/
- Google Navigation pour Android 2.0
  - Le marché des GPS va-t-il mourir ?
    - http://www.macworld.com/article/143547/2009/10/android_turnbyturn.html
- Google Gears remplacé par HTML 5 ?
  - http://latimesblogs.latimes.com/technology/2009/11/google-gears.html

Actualité

- Sortie de Metasploit 3.3
  - Des nouveautés majeures
    - Support Windows Seven, systèmes 64 bits, Oracle, MS-SQL, etc.
    - Payloads JSP
    - Ecoute du réseau "tout en mémoire" sous Windows
    - Détection des stations DECT et écoute des conversations
    - Etc. etc.

    - http://www.metasploit.com/framework/download/

- Sortie de Metasploit 3.3.1 (15 jours plus tard)
  - Intégration avec Rapid7 NeXpose

- Sortie de Nessus 4.2
  - Nouvelle interface entièrement en Flash (!)

- Un projet d'ampleur pour casser A5/1
    - http://spectrum.ieee.org/telecom/wireless/open-source-effort-to-hack-gsm

Actualité

- **HP rachète 3Com pour 2,7 Md$**
  - **Et accessoirement le programme TippingPoint/ZDI**
    - **http://www.zdnet.fr/blogs/cloud-news/hp-s-offre-3com-pour-27-milliards-de-dollars-39710678.htm**

- **IBM achète Guardium**
  - **Un logiciel de protection des bases de données**
    - **http://www.guardium.com/index.php/pr/923**

- **La norme ISO 29147**
  - **... encadre le *Responsible Disclosure***
    - **http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=45170**

Actualité

- SCADA FAIL
  - Résumé de l'épisode précédent
    - Les "hackers" ne sont pas responsables des pannes électriques à répétition au Brésil
  - Mais à force de répéter que c'est possible
    - Des gens ont fini par le faire !
      - http://news.slashdot.org/story/09/11/17/2245241/Hackers-Broke-Into-Brazil-Grid-Last-Thursday
- Le racket de la base client de Belgacom prend fin
  - L'auteur a été arrêté: il a 20 ans
    - http://www.7sur7.be/7s7/fr/3007/Bruxelles/article/detail/1037253/2009/12/03/Le-hacker-Vendetta-sous-mandat-d-arret-apres-ses-aveux.dhtml
- Fortinet entre au Nasdaq
    - http://bourse.trader-finance.fr/Fortinet+annonce+son+introduction+sur+le+Nasdaq+358929

Fun

- La société PrevX humiliée
  - Annonce un problème avec les mises à jour Microsoft du mois de novembre
    - http://www.prevx.com/blog/140/Black-Screen-woes-could-affect-millions-on-Windows--
    - Vista-and-XP.html
  - ... sauf que le problème provient du poste de l'utilisateur chez PrevX
    - http://www.pcinpact.com/actu/news/54400-windows-ecrans-noirs-prevx-faute.htm
    - http://blogs.technet.com/msrc/archive/2009/12/01/reports-of-issues-with-november-security-updates.aspx
    - http://www.prevx.com/blog/142/Windows-Black-Screen-recap.html
  - Cela fait réfléchir sur le traitement de l'information et des failles aujourd'hui !
- Shodan: la recherche par port TCP + bannière
  - Un monde de possibilités ...
    - http://shodan.surtri.com/?q=port%3A23+List+of
- Moins dangereux ... mais rigolo quand même
    - http://www.google.com/search?q=filetype%3Apdf+file+c

Fun

- Des shellcodes ... uniquement en anglais
  - http://www.cs.jhu.edu/~sam/ccs243-mason.pdf
- D'où viennent les systèmes d'exploitation utilisés dans les films ?
  - http://blog.coleran.com/category/portfolio/screendesign
- Enfin une vraie sécurité: le lecteur d'esprit
  - http://www.brainwavescience.com/
- Un hacker au Vatican
  - Frère Bruno
    - http://www.zenit.org/rssfrench-22662

Questions / réponses

- Questions / réponses
- Prochaine réunion
  - Mardi 12 janvier 2010
  - Assemblée générale de l'association le matin
    - Il est possible d'adhérer sur place
    - Venez nombreux !
- N'hésitez pas à proposer des sujets et des salles