OSSIR
Groupe Paris

Réunion du 13 juillet 2010

Revue des dernières vulnérabilités

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

Avis Microsoft

- **Prévisions pour Juillet 2010**
  - **4 bulletins, 5 failles**
    - **2 bulletins critiques affectant Windows**
    - **1 bulletin critique et 1 bulletin important dans Office**
    - **http://blogs.technet.com/b/msrc/archive/2010/07/08/july-2010-bulletin-release-advance-notification.aspx**
  - **MS10-042 va corriger l'avis « Help Center »**
  - **MS10-043 va corriger « Canonical Display Driver »**
- **Advisories**
  - **Q2219475 Faille dans « Windows Help & Support »**
    - **V1.2: la faille commence à être exploitée dans la nature**

Avis Microsoft

- **Une liste (non exhaustive) des failles non corrigées affectant des produits Microsoft à ce jour**
  - **Elévation de privilèges locale dans Windows Vista/2008**
    - **http://www.securityfocus.com/bid/41280/info**
  - **Contournement de l'authentification « htaccess » sur IIS 5.1**
    - **http://soroush.secproject.com/blog/2010/07/iis5-1-directory-authentication-bypass-by-using-i30index_allocation/**
  - **Fuite d'information sur le layout mémoire d'Internet Explorer**
    - **Via CTimeoutEventList::InsertIntoTimeoutList [MSHTML.DLL]**
    - **http://reversemode.com/index.php?option=com_content&task=view&id=68&Itemid=1**
  - **Faille dans l'API UpdateFrameTitleForDocument() [MFC42.DLL]**
    - **Exploitable via certaines applications, comme PowerZip**
    - **http://secunia.com/advisories/40298/**
  - **CSRF dans OWA 2007**
    - **http://sites.google.com/site/tentacoloviola/pwning-corporate-webmails**

Avis Microsoft

- Révisions
  - MS09-040
    - V1.1: ajout d'un problème connu
  - MS09-061
    - V1.4: .NET 1.1 n'est pas disponible sur Windows Seven/2008 R2
  - MS10-016
    - V2.1: correction des paramètres de ligne de commande
    - V2.2: correction des paramètres de ligne de commande
  - MS10-026
    - V1.1: changement de la logique de détection
  - MS10-033
    - V1.2: ajout de problèmes documentés, correction du *workaround*
    - V1.3: correction du nom d'une clé de BdR

Avis Microsoft

- MS10-035
  - V1.1: correction du *workaround*
- MS10-036
  - V1.1: correction d'un nom de fichier
- MS10-038
  - V1.2: ajout d'un problème connu
- MS10-040
  - V1.1: ajout d'un problème connu
- MS10-041
  - V1.1: correction du nom d'une clé de BdR
  - V1.2: changement de la logique de détection
  - V1.3: correction du nom d'une clé de BdR

Infos Microsoft

- Sorties logicielles
  - Exchange 2007 SP3
    - Permet d'installer Exchange 2007 sur Windows 2008 R2
  - Mise à jour « non sécurité »
    - Préalable au déploiement de .NET 4
      - http://support.microsoft.com/kb/982524
  - La dernière version de Messenger n'est pas compatible Windows XP
      - http://www.windowslive.fr/messenger/nouveautes/
- Autre
  - Fin de vie pour Windows 2000 et XP SP2

Infos Réseau

- (Principales) faille(s)
  - 15 failles corrigées dans Cisco ASA < 8.1(2)
    - http://www.cisco.com/en/US/docs/security/asa/asa81/release/notes/asarn812.html
  - Comodo informe publiquement VeriSign d'une faille dans la génération de ses certificats
    - http://www.comodo.com/news/press_releases/2010/06/comodo-informs-verisign-security-vulnerability.html

Infos Réseau

- **Autres infos**
  - **Attaques en brute-force SSH**
    - **Vous avez pensé à « PasswordAuthentication no »**
    - **Mais avez-vous pensé à « ChallengeResponseAuthentication no » ?**
      - **http://isc.sans.edu/diary.html?storyid=9034**
  - **iOS 4 supporte IPv6**
      - **http://isc.sans.edu/diary.html?storyid=9058**
    - **Enfin … pas sans IPv4**
      - **http://lists.apple.com/archives/ipv6-dev/2010/Jun//msg00036.html**
  - **Le serveur racine « i » passe en IPv6**
      - **http://ops.ietf.org/lists/v6ops/v6ops.2010/msg00760.html**

Infos Unix

- **(Principales) faille(s)**
  - **Sudo**
    - **Contournement du « secure path » en définissant 2 variables « PATH »**
      - **http://www.sudo.ws/sudo/alerts/secure_path.html**
  - **Samba < 3.3.12**
    - **Corruption mémoire « classique »**
      - **http://www.samba.org/samba/security/CVE-2010-2063.html**
      - **http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=873**
  - **LibPNG < 1.2.44, < 1.4.3**
    - ***Buffer overflow***
      - **http://www.libpng.org/pub/png/libpng.html**
  - **LibTIFF < 3.9.4**
    - **Débordement(s) d'entier(s)**
      - **http://www.remotesensing.org/libtiff/v3.9.3.html**
      - **http://www.remotesensing.org/libtiff/v3.9.4.html**
      - **http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=874**

Infos Unix

- CUPS < 1.4.4
  - Plusieurs failles corrigées
    - http://cups.org/articles.php?L596
- MySQL < 5.1.48
  - Déni de service
    - http://dev.mysql.com/doc/refman/5.1/en/news-5-1-48.html
- ISC DHCPd
  - Déni de service
    - http://www.isc.org/software/dhcp/advisories/cve-2010-2156
- Pmount
  - « Symlink Attack »
    - http://www.debian.org/security/2010/dsa-2063
- Apache mod_proxy_http 2.2.x
  - Fuite de données lors d'un *timeout*
    - CVE-2010-2068

Infos Unix

- **Bogofilter < 1.2.2**
  - ***Buffer overflow* dans le décodeur Base64**
    - **http://www.certa.ssi.gouv.fr/site/CERTA-2010-AVI-301/CERTA-2010-AVI-301.html**
- **PAM sur Ubuntu 9 et 10**
  - **Elévation de privilèges locale (triviale)**
    - **http://www.ubuntu.com/usn/usn-959-1**
- **Ruby < 1.9.1p429**
  - ***Buffer overflow* dans l'API « ARGF.inplace_mode »**
    - **http://www.ruby-lang.org/en/news/2010/07/02/ruby-1-9-1-p429-is-released**
- **Rpc.ttdbserverd sur AIX, Solaris et HP/UX**
  - ***Heap overflow***
    - **http://archives.neohapsis.com/archives/fulldisclosure/2010-07/0199.html**
- **Des vulnérabilités dans OpenVMS**
  - **Suffisamment rare pour être signalé ☺**
    - **http://www.certa.ssi.gouv.fr/site/CERTA-2010-AVI-297/CERTA-2010-AVI-297.html**
- **Déni de service sur XenServer**
  - **Affecte: 5.0 et 5.5**
    - **http://support.citrix.com/article/CTX125319**

Infos Unix

- Autre
  - Le retour d'OS/2 ?
    - http://www.linuxjournal.com/content/new-os2-rumours-could-be-interesting

Failles

- **Principales applications**
  - **Mac OS X < 10.6.4**
    - **28 failles corrigées**
      - **http://support.apple.com/kb/HT4188**
  - **iTunes < 9.2**
    - **40 failles corrigées**
      - **http://support.apple.com/kb/HT4220**
  - **iOS (iPhone OS) < 4**
    - **65 failles corrigées**
      - **http://support.apple.com/kb/HT4225**
    - **Note: les découvreurs des failles sont crédités par Apple**
  - **Thunderbird < 3.0.5**
    - **Corrige mfsa2010-25, mfsa2010-26, mfsa2010-29, mfsa2010-30**
  - **Thunderbird 3.1 est disponible**
    - **Bogues corrigés ?**

Failles

- FireFox < 3.5.10, < 3.6.6
  - Corrige mfsa2010-25 … mfsa2010-33
    - Ainsi que ZDI-10-113
  - Et intègre les « bac à sable » pour plugins
    - http://www.clubic.com/navigateur-internet/mozilla-firefox/actualite-348656-firefox-crash-plantages-plugin-flash.html
  - Attention, par défaut FireFox utilise désormais le même proxy que IE

- Chrome < 5.0.375.99
    - http://googlechromereleases.blogspot.com/2010/06/stable-channel-update.html
    - http://googlechromereleases.blogspot.com/2010/06/stable-channel-update_24.html
    - http://googlechromereleases.blogspot.com/2010/07/stable-channel-update.html

- Opera < 10.60
    - http://www.opera.com/docs/changelogs/windows/1054/
    - http://www.opera.com/docs/changelogs/windows/1060/
    - http://www.opera.com/support/kb/view/954/
    - http://www.opera.com/support/kb/view/955/
    - http://www.opera.com/support/kb/view/957/
    - http://www.opera.com/support/kb/view/958/
  - Intègre également une liste d'URL malveillantes fournie par AVG

Failles

- Adobe Reader < 8.2.3, < 9.3.3
  - 17 failles corrigées
    - http://www.adobe.com/support/security/bulletins/apsb10-15.html
    - http://secunia.com/secunia_research/2010-74/
    - http://secunia.com/secunia_research/2010-88/
    - http://www.zerodayinitiative.com/advisories/ZDI-10-116/
  - Crédits
    - Nicolas Joly / VUPEN (x4)
    - MSVR
    - Didier Stevens
    - Philippe Lagadec / OTAN
    - Anonymous / ZDI
    - James Quirk / Los Alamos
    - Gjoko Krstic / Zero Science Lab
    - Alin Rad Pop / Secunia
    - Carsten Eiram / Secunia
    - Tavis Ormandy / Google (x5)
  - Note: la fonction « LaunchAction » n'est pas supprimée
    - http://blog.bkis.com/en/adobe-fix-still-allows-escape-from-pdf/
    - http://www.h-online.com/security/news/item/Adobe-s-protection-against-embedded-scripts-incomplete-1033144.html

Failles

- Flash < 10.1
  - Précision par rapport au mois dernier
    - Corrige également ZDI-10-109, ZDI-10-110, ZDI-10-111, ZDI-10-114 et ZDI-10-115
- Adobe va-t-il raccourcir son cycle de mise à jour ?
  - http://www.h-online.com/security/news/item/Adobe-considers-shorter-update-cycles-1009131.html
- Exploitation d'une faille multi-navigateurs
  - Grâce à « about:blank »
    - http://lcamtuf.blogspot.com/2010/06/yeah-about-that-address-bar-thing.html
- Wireshark < 1.2.9
    - http://www.wireshark.org/security/wnpa-sec-2010-05.html
    - http://www.wireshark.org/security/wnpa-sec-2010-06.html

Failles

- Patch pour ESX 3.5
  - 321 Mo …
    - http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1022899
- Les failles Oracle du mois de juillet
  - 59 failles dont 21 affectant Solaris
    - http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2010.html
  - « Oracle Secure Backup » n'est pas si « *secure* » que ça …
    - ZDI-10-118, ZDI-10-119, ZDI-10-120, ZDI-10-121, ZDI-10-122, ZDI-10-123, ZDI-10-124
    - http://dvlabs.tippingpoint.com/advisory/TPTI-10-04
    - http://www.vsecurity.com/resources/advisory/20100713-1/

Failles

- Failles Java: IBM suit son propre cycle de correctifs
  - http://www.ibm.com/developerworks/java/jdk/alerts/
- Un nombre considérable de failles corrigées dans la gamme Xerox WorkCenter
  - En vue d'une certification « critères communs »
    - http://www.xerox.com/downloads/usa/en/c/cert_XRX10-003_v1.0.pdf
- DEP et ASLR dans les logiciels grand public, c'est pas fait
  - http://secunia.com/gfx/pdf/DEP_ASLR_2010_paper.pdf
- Les produits Apple ont plus de failles de sécurité que les produits Microsoft ou Oracle
  - D'après une étude sérieuse de Secunia
    - http://secunia.com/gfx/pdf/Secunia_Half_Year_Report_2010.pdf
- Sortie de Metasploit 3.4.1
  - Avec un meterpreter pour PHP
    - http://blog.metasploit.com/2010/07/metasploit-framework-341-released.html

Failles 2.0

- XSS permanent sur YouTube
  - http://isc.sans.edu/diary.html?storyid=9130
- Le patron sécurité de Facebook demande à être piraté par ses employés
  - Ils attaquent son WiFi domestique
    - http://techcrunch.com/2010/07/05/employees-challenged-to-crack-facebook-security-succeed/
- The Pirate Bay … piraté
  - 4 millions de comptes volés par un injection SQL
    - http://krebsonsecurity.com/2010/07/pirate-bay-hack-exposes-user-booty/
- Collecte d'informations classifiées …
  - Via de faux profils Facebook / LinkedIn
    - http://www.darkreading.com/insiderthreat/security/privacy/showArticle.jhtml?articleID=225702468

Failles 2.0

- Les « *rogue antivirus* » arrivent … par un appel téléphonique
  - http://www.pcpro.co.uk/news/security/359233/the-unstoppable-tech-support-scam
  - http://www.pcpro.co.uk/news/security/356833/pensioner-targeted-by-fake-virus-phone-scam
- Le « pirate » qui avait eu accès aux précommandes d'iPad a été arrêté
  - … pour possession de drogue
    - http://www.theregister.co.uk/2010/06/16/auernheimer_arrested/
- Les précommandes d'iPhone 4 aussi piratées chez AT&T (!)
  - http://gizmodo.com/5564262/apple-iphone-4-order-security-breach-exposes-private-information

Malwares et spam

- Un nouveau site pour lutter contre la fraude sur Internet
  - De nombreux partenaires, dont Microsoft, eBay, Paypal, …
    - http://ifraudalert.org/
- 13 failles découvertes dans des « packs » d'exploitation Web
  - Les pirates ne sont pas meilleurs que les autres ☺
    - http://www.tehtri-security.com/en/news.php#news-39
- Le site Lenovo.com infecté
    - http://cyberinsecure.com/lenovo-support-website-loads-malicious-iframe-infects-visitors-with-trojan/
- Les téléphones portables, un nid à virus ?
  - Oui … d'après un vendeur d'antivirus
    - http://www.netqin.com/en/security/newsinfo_2841_1.html

Actualité (francophone)

- Rapport du CLUSIF « Menaces et Pratiques de Sécurité »
  - Conclusion: la sécurité peine à avancer en France
    - http://www.clusif.asso.fr/fr/infos/event/#conf100617
- L'exercice « Piranet 2010 » s'est passé
    - http://www.ssi.gouv.fr/IMG/pdf/2010-06-25_Communique_de_presse_Piranet_2010.pdf
- Bilan de la consultation publique sur la « neutralité du net »
    - http://www.telecom.gouv.fr/fonds_documentaire/consultations/10/synthese-consultation-neutralitenet.pdf
- Le gouvernement s'attaque au « *ping call* »
    - http://www.economie.gouv.fr/presse/dossiers_de_presse/100621spam.pdf
- Les rencontres de la modernisation de l'Etat
    - http://www.acteurspublics.com/rmde-2010

Actualité (francophone)

- **Inauguration du Laboratoire de Haute Sécurité de l'INRIA**
  - **http://www.inria.fr/nancy/actualites/inauguration-du-laboratoire-de-haute-securite-informatique**
- **TERA 100 entre en service**
  - **http://www.strategiestm.com/Le-supercalculateur-le-plus.html**
- **La DIRISI signe un contrat cadre avec Microsoft**
  - **http://questions.assemblee-nationale.fr/q13/13-75878QE.htm**
- **VUPEN ne « donnera » plus ses failles à Microsoft**
  - **http://www.vupen.com/english/threats/**
  - **http://www.h-online.com/security/news/item/Microsoft-vulnerabilities-full-disclosure-and-no-disclosure-1033551.html**

Actualité (francophone)

- Publications de la CNIL
  - Le guide du droit d'accès aux données personnelles
    - http://www.cnil.fr/fileadmin/documents/Guides_pratiques/CNIL_Droit_d_acces.pdf
  - Observations sur la LOPPSI
    - http://www.cnil.fr/fileadmin/documents/Communications/NOTE_D-OBSERVATIONS_LOPPSI_06-05-2010.pdf
  - Rapport d'activité 2009
    - http://www.cnil.fr/uploads/media/CNIL-30erapport_2009.pdf
  - Les smartphones en question
    - http://www.cnil.fr/la-cnil/actu-cnil/article/article/2/les-smartphones-en-questions/
    - Je suppose que la CNIL veut dire « ordiphones » ☺

Actualité (francophone)

- **HADOPI se met en marche**
  - **Les premiers emails devraient être envoyés autour du 21 juin 2010**
  - **La CNIL donne son aval**
    - **Seule la société « Trident Media Guard » sera autorisée à collecter des adresses IP**
  - **Mais reste réticente …**
    - **http://www.20minutes.fr/article/579769/vous-interviewez-Vous-avez-interviewe-Yann-Padova-secretaire-general-de-la-Cnil.php**
- **Echec pour le logiciel de sécurisation « HADOPI » proposé par Orange**
  - **http://seclists.org/fulldisclosure/2010/Jun/346**

Actualité (anglo-saxonne)

- A quoi ressemble un « cyber état d'urgence » ?
  - http://www.pcinpact.com/actu/news/57587-cyber-securite-president-pouvoir-urgence.htm
- Le programme « Citoyen Parfait »
  - Un sniffer gouvernemental dans chaque réseau SCADA
  - Est-ce une si bonne idée ?
    - http://www.lemonde.fr/technologies/article/2010/07/08/citoyen-parfait-le-big-brother-a-l-americaine_1385055_651865.html
- Marc Maiffret retourne chez eEye
  - http://news.cnet.com/8301-27080_3-20010339-245.html
- Les Australiens réfléchissent à des mesures de sécurisation « drastiques » pour Internet
  - Déconnexion des machines infectées
  - Responsabilité financière des éditeurs en cas de faille de sécurité
  - Etc.
    - http://www.news.com.au/technology/no-anti-virus-software-no-internet-connection/story-e6frfro0-1225882656490

Actualité (anglo-saxonne)

- Pas d'iPhone professionnel pour les fonctionnaires anglais
  - Seul le BlackBerry est autorisé
    - http://www.networkworld.com/news/2010/061710-no-iphones-just-blackberries-for.html
- Fin de vie pour Cisco CSA
    - http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5739/ps2330/end_of_life_c51-602579.html
- Un challenge de social engineering à DefCon
    - http://www.csoonline.com/article/598614/defcon-contest-to-spotlight-social-engineering?page=1
- La conférence ReCON 2010 a eu lieu

Actualité (européenne)

- Première pour HITB Europe
  - Plusieurs conférences intéressantes
    - http://archives.neohapsis.com/archives/fulldisclosure/2010-07/0064.html
  - Mais une couverture médiatique assez faible

Actualité (Google)

- Android 2.2 disponible
  - 100% Open Source
    - http://android-developers.blogspot.com/2010/06/froyo-code-drop.html
- Résultat de l'inspection CNIL
  - Google a bien enregistré du trafic POP3/SMTP en clair sur des points d'accès WiFi
    - http://www.macbidouille.com/news/2010/06/18/les-voitures-street-view-ont-enregistre-des-mails
  - (Qui est à blâmer ?)
- Google transige avec la Chine
  - Pour ne pas perdre sa licence d'opérateur Internet
    - http://www.google.com/hostednews/afp/article/ALeqM5h6pLEgrySWljQChQ2gI-ngesEQKw

Actualité (Google)

- Chrome OS prévu pour l'automne
  - http://www.developpez.net/forums/d836884/club-professionnels-informatique/actualites/version-finale-chrome-os-sortira-lautomne-2010-pourrait-passer-cloud-client-leger/
- Google Me
  - Le futur nouveau réseau social de Google ?
- Les outils Google … en ligne de commande
  - http://code.google.com/p/googlecl/

Actualité

- Sorties logicielles
  - OWASP O2 (première beta)
    - Une plateforme de développement et d'audit collaboratif pour applications Web
    - http://diniscruz.blogspot.com/2010/07/first-major-release-of-owasp-o2.html
  - Qubes (alpha 2)
    - http://theinvisiblethings.blogspot.com/2010/07/qubes-alpha-2-released.html
  - L'EFF propose le plugin « HTTPS everywhere »
    - Attention aux effets d'annonce toutefois: HTTPS n'est pas l'arme absolue !
    - https://www.eff.org/https-everywhere
  - REMnux
    - Une distribution Linux dédiée à l'analyse de malwares
      - http://zeltser.com/remnux/
  - Python 2.7
    - Avec un support étendu à 5 ans
    - http://www.python.org/download/releases/2.7/

Actualité

- Le chiffrement Skype révélé
  - Une conférence au CCC à venir
    - http://cryptolib.com/ciphers/skype/
    - http://securitewifi.fr/wifi/2010/07/12/les-secrets-du-chiffrement-de-skype-reveles/
- GFI rachète SunBelt
- Les budgets sécurité pourraient diminuer en 2011
  - Source: Gartner
    - http://www.cnis-mag.com/budgets-securite-en-recul-pour-2011.html
- Les choses dont on a déjà parlé à l'OSSIR
  - Security Garden est désormais en ligne
    - https://www.securitygarden.com/
  - Suricata 1.0.0
    - http://www.openinfosecfoundation.org/

Fun

- La guerre des tablettes aura bien lieu
  - Cisco Cius
    - http://www.cisco.com/en/US/products/ps11156/index.html
- Le pare-feu OpenOffice
  - Il existe bel et bien !
    - http://www.wzdftpd.net/blog/index.php?2010/06/16/46-le-pare-feu-openoffice

Questions / réponses

- Questions / réponses
- Prochaine réunion
  - Mardi 14 septembre 2010
- N'hésitez pas à proposer des sujets et des salles