OSSIR
Groupe Paris

Réunion du 12 juillet 2011

Revue des dernières vulnérabilités

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

Avis Microsoft

- **Juin 2011**
  - **16 bulletins, 34 failles**
    - **http://blogs.technet.com/b/srd/archive/2011/06/14/assessing-the-risk-of-the-june-security-updates.aspx**
  - **MS11-037 Faille dans le support mhtml:// [3]**
    - **Affecte: Windows (toutes versions supportées)**
    - **Exploit:**
      - **"Fuite d'information" (XSS)**
      - **Remplace MS11-026**
    - **Crédit: n/d**

Avis Microsoft

- MS11-038 Faille WMF [1]
  - Affecte: Windows (toutes versions supportées)
  - Exploit: exécution de code arbitraire depuis OLE Automation
    - "Underflow"
  - Crédit: Yamati Li / Palo Alto Networks

- MS11-039 Faille .NET [1]
  - Affecte: .NET & SilverLight (toutes versions supportées)
    - Sauf SilverLight 4, .NET 1.1 SP1, .NET 3.0 et .NET 3.0 SP1
  - Exploit: exécution de code hors de la sandbox
    - http://weblog.ikvm.net/PermaLink.aspx?guid=4eb904a7-e81d-4340-8258-f23835441242
  - Crédit: Michael J. Liu

Avis Microsoft

- MS11-040 Faille dans ForeFront TMG [1]
  - Affecte: ForeFront TMG 2010
  - Exploit: exécution de code arbitraire si le pare-feu communique avec un client malveillant
    - Fonction interne NSPLookupServiceNext()
  - Crédit: n/d
- MS11-041 Faille dans le support OTF [2]
  - Affecte: Windows (toutes versions supportées en 64 bits)
  - Exploit: exécution de code en mode noyau à l'ouverture d'une police
    - Exploitable à distance dans IE (!)
  - Crédit: Koro / www.korosoft.net

Avis Microsoft

- **MS11-042 Failles dans DFS [1,3]**
  - **Affecte: Windows (toutes versions supportées, sauf Seven SP1 et 2008R2 SP1)**
  - **Exploit:**
    - **Exécution de code, déni de service**
      - **… si un client se connecte à un serveur malveillant**
  - **Crédit: Laurent Gaffié / NGS Software**

- **MS11-043 Faille SMB [1]**
  - **Affecte: Windows (toutes versions supportées)**
  - **Exploit: exécution de code**
    - **… si un client se connecte à un serveur malveillant**
  - **Crédit: n/d**

Avis Microsoft

- MS11-044 Faille .NET [2]
  - Affecte: .NET(toutes versions supportées)
    - Sauf .NET 1.1 SP1, .NET 3.0 et .NET 3.0 SP1
  - Exploit: exécution de code en dehors de la sandbox (?)
    - A cause de l'optimiseur JIT
    - http://blogs.technet.com/b/srd/archive/2011/06/14/ms11-044-jit-compiler-issue-in-net-framework.aspx
  - Crédit: Dan Kaminsky (pour avoir signalé que MD2 ne doit plus être utilisé)

- MS11-045 Failles dans Excel (x8) [1…3]
  - Affecte: Office (toutes versions supportées, y compris Viewer, Converter, et Mac)
    - Mais pas Works 9
  - Exploit: exécution de code à l'ouverture d'un fichier Excel malformé
  - Crédit:
    - Bing Liu / Fortinet
    - Anonymous / iDefense (x2)
    - Nicolas Gregoire / Agarri
    - Omair (x2)
    - Will Dormann of the CERT/CC (x2)

Avis Microsoft

- **MS11-046 Faille dans AFD.SYS [1]**
  - Affecte: Windows (toutes versions supportées)
  - Exploit: élévation de privilèges
  - Crédit:
    - Steven Adair / Shadowserver Foundation
    - Chris S.

- **MS11-047 Faille dans Hyper-V [3]**
  - Affecte: Hyper-V (Windows 2008 et 2008R2)
  - Exploit: déni de service de l'hôte par un invité
  - Crédit: Nicolas Economou / CORE

Avis Microsoft

- MS11-048 Faille dans le serveur SMB [3]
  - Affecte: Windows Vista, 2008, Seven, 2008R2
  - Exploit: déni de service
  - Crédit: n/d

- MS11-049 Fuite d'information dans l'éditeur XML [3]
  - Affecte:
    - Editeur InfoPath >= 2007
    - Editeur SQL Server >= 2005
    - Editeur Visual Studio >= 2005
  - Exploit: abus des "XML External Entities"
    - A l'ouverture d'un fichier ".disco"
  - Crédit: Jesse Ou / Cigital

Avis Microsoft

- MS11-050 Failles IE (x11) [1…3]
  - Affecte: IE (toutes versions supportées)
  - Exploit:
    - Fuite d'information, exécution de code à l'ouverture d'une page malformée
      - ZDI-11-193 … ZDI-11-198
      - ZDI-11-198 = faille utilisée lors du concours pwn2own
      - http://blogs.technet.com/b/srd/archive/2011/06/14/ms11-050-ie9-is-better.aspx
      - http://labs.m86security.com/2011/06/0-day-exploit-used-in-a-targeted-attack-cve-2011-1255/
      - http://d0cs4vage.blogspot.com/2011/06/insecticides-dont-kill-bugs-patch.html

Avis Microsoft

- Crédit:
  - Robert Swiecki / Google Inc.
  - NSFOCUS
  - Anonymous / Beyond Security Secure Disclosure program
  - Adi Cohen / IBM Rational Application Security
  - Trend Micro
  - Nirmal Singh Bhary / Norman
  - Anonymous / iDefense
  - Damian Put / ZDI
  - Yoel Gluck, Yogesh Badwe, Varun Badhwar / salesforce.com Product Security
  - Jose Antonio Vazquez Gonzalez / ZDI
  - Anonymous / ZDI
  - Peter Winter-Smith / ZDI
  - Stephen Fewer / Harmony Security + ZDI

Avis Microsoft

- MS11-051 Faille dans AD Certificate Services Web Enrollment [1]
  - Affecte: Windows (toutes versions serveur)
  - Exploit: XSS
  - Crédit:
    - Ruggero Strabla / Emaze Networks
    - Saipem Security Team

- MS11-052 Faille le support VML par IE [1]
  - Affecte: IE (toutes versions supportées, sauf IE9)
  - Exploit: exécution de code à l'ouverture d'un fichier VML malformé dans IE
  - Crédit: Anonymous /ZDI

Avis Microsoft

- Advisories
  - Q2501584 "Office File Validation"
    - V2.0: mise à disposition dans Microsoft Update
  - Note: évasion du mode protégé dans Office 2010 …
    - http://weblog.ikvm.net/PermaLink.aspx?guid=d2db3fc7-46e0-40ff-92b8-65702f155c32
  - Q2524375 Certificats frauduleux
    - V5.0: révocation sur Zune HD

Avis Microsoft

- Révisions
  - MS11-025
    - V3.0: nouveau correctif pour Visual 2005 SP1, 2008 SP1 et 2010
  - MS11-028
    - V2.1: mise à jour de la logique de détection
    - V2.2: corrections documentaires
  - MS11-036
    - V1.2: le correctif pour Mac est disponible dans MS11-045
      - Et corrections de clés de base de registre pour Office File Validation
  - MS11-042
    - V1.1: Windows 7 SP1 et 2008R2 SP1 ne sont pas affectés
  - MS11-043
    - V1.1: ajout d'un problème connu (avec Samba)
  - MS11-046
    - V1.1: cette mise à jour remplace MS10-058
  - MS11-049
    - V1.1: suppression d'entrées dans la table des logiciels non affectés
    - V1.2: suppression d'entrées dans la table des logiciels non affectés
    - V1.3: corrections documentaires
  - MS11-051
    - V1.1: précisions documentaires sur le filtre anti-XSS

Infos Microsoft

- Sorties logicielles
  - Office 365 (RTM)
    - http://www.microsoft.com/Presspass/press/2011/jun11/06-28MSOffice365PR.mspx
  - Office 2010 SP1 (RTM)
  - IE 10 (Platform Preview 2)
    - http://www.winbeta.org/?q=news/microsoft-releases-ie10-platform-preview-2
  - Fin de vie pour Vista SP1 … aujourd'hui !

Infos Microsoft

- Autre
  - Office BPOS: 3h de panne
    - Pas glop pour une solution en ligne
  - Le brevet de Microsoft sur l'interception légale de la VoIP fait couler de l'encre
    - http://yro.slashdot.org/story/11/06/27/1553216/Microsoft-May-Add-Eavesdropping-To-Skype
  - Windows Thin PC
    - http://www.microsoft.com/windows/enterprise/solutions/virtualization/products/thinpc.aspx

Infos Réseau

- (Principales) faille(s)
  - BIND < 9.8.0-P4
    - Déni de service (x2)
      - http://www.isc.org/advisories/bind
      - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2464
      - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2465
  - Cisco Content Gateway
    - "*Unexpected reload*" suite à un ICMP malformé …
      - http://www.cisco.com/warp/public/707/cisco-sa-20110706-csg.shtml
  - Arkoon FAST360 VPN
    - Faille non publique …
      - https://support-https.arkoon.net/security/advisories.php
  - Avaya IP Office et Branch Gateway
    - "*Directory traversal*" dans le serveur TFTP
      - https://support.avaya.com/css/P8/documents/100141179

Infos Réseau

- **Autres infos**
  - **Tous les TLD sont désormais possibles**
    - **http://www.zdnet.fr/actualites/nouvelles-extensions-de-domaines-a-partir-2012-a-decide-l-icann-39761784.htm**
    - **http://lexpansion.lexpress.fr/high-tech/lancement-de-nouveaux-noms-de-domaine-pour-les-entreprises_257342.html**

Infos Unix

- (Principales) faille(s)
  - Faille dans OpenSSH 3.4
    - Affecte: FreeBSD
    - Exploit: exécution de code à distance avant authentification ☺
      - http://archives.neohapsis.com/archives/fulldisclosure/2011-07/0006.html
      - http://twitter.com/#!/msfriedl/status/87114829789278208
  - Plusieurs plugins Wordpress backdoorés
      - http://wordpress.org/news/2011/06/passwords-reset/
      - http://adamharley.co.uk/2011/06/wordpress-plugin-backdoors/
  - phpMyAdmin < 3.3.10.2, < 3.4.3.1
    - Failles exploitables (sous conditions)
      - http://ha.xxor.se/2011/07/phpmyadmin-3x-multiple-remote-code.html
  - PHP <= 5.3.6
    - Contournement des filtres d'*upload*
      - http://svn.php.net/viewvc?view=revision&revision=312103
      - http://blog.kotowicz.net/2011/06/file-path-injection-in-php-536-file.html

Infos Unix

- Wordpress < 3.1.4
  - http://wordpress.org/news/2011/06/wordpress-3-1-4/
- Joomla! < 1.6.4
  - http://developer.joomla.org/security/news/350-20110603-unauthorised-access.html
- Drupal
  - http://drupal.org/node/1204582
- Zope/Plone
  - http://plone.org/products/plone/security/advisories/20110622
- DokuWiki
  - XSS dans le générateur de flux RSS
    - http://www.freelists.org/post/dokuwiki/Hotfix-Release-20110525a-Rincewind

- LibreOffice < 3.3.3, < 3.4.0
  - Failles lors de l'ouverture d'un fichier "Lotus Word Pro"
    - http://www.kb.cert.org/vuls/id/953183

- Libcurl
  - Réflexion d'authentifiants GSSAPI
    - http://curl.haxx.se/docs/adv_20110623.html

Infos Unix

- **Autre**

  - **Vsftpd "backdooré"**
    - **Suite à la compromission de l'hébergeur**
      - **http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html**

  - **Des failles dans le Cloud Open Source "Eucalyptus"**
      - **http://www.bulletins-electroniques.com/actualites/66982.htm**

Failles

- **Principales applications**
  - Adobe Flash Player < 10.3.181.26
    - http://www.adobe.com/support/security/bulletins/apsb11-18.html
    - http://blogs.technet.com/b/mmpc/archive/2011/07/01/a-technical-analysis-on-the-exploit-for-cve-2011-2110-adobe-flash-player-vulnerability.aspx
    - Note: Blitzableiter 1.0 est sorti
      - http://blitzableiter.recurity.com/projects/show/blitzableiter
      - http://blogs.adobe.com/asset/2011/06/examples-of-community-engagement.html
  - Adobe Reader < 10.1 (x13)
    - ZDI-11-218, ZDI-11-219
      - http://www.adobe.com/support/security/bulletins/apsb11-16.html
  - Adobe ColdFusion (x2)
    - APSB11-14
  - Adobe LifeCycle * (x2)
    - APSB11-15
  - Adobe ShockWave Player (x24 !)
    - APSB11-17
    - ZDI-11-200 … ZDI-11-217, ZDI-11-220 , ZDI-11-221 , ZDI-11-222
    - TPTI-11-07 … TPTI-11-11

Failles

- FireFox < 3.6.18, < 5.0
  - ZDI-11-223, ZDI-11-224, ZDI-11-225
    - http://www.mozilla.org/security/known-vulnerabilities/firefox.html#firefox5
- Thunderbird < 3.1.11, < 5.0
    - http://www.mozilla.org/security/known-vulnerabilities/thunderbird31.html#thunderbird3.1.11
  - Note: le passage rapide de Mozilla 4.0 à 5.0 fait jaser …
    - http://www.securityvibes.fr/marche-business/firefox-4-microsoft-internet-explorer/
- Chrome < 12.0.742.112
    - http://googlechromereleases.blogspot.com/2011/06/stable-channel-update_28.html
- Opera < 11.50
    - http://www.opera.com/docs/changelogs/windows/1150/
    - http://www.opera.com/support/kb/view/995/
    - http://www.opera.com/support/kb/view/996/
- Oracle Quaterly Patch, juin 2011 (suite)
  - ZDI-11-182 … ZDI-11-192, ZDI-11-199
  - TPTI-11-06
    - http://www.oracle.com/technetwork/topics/security/javacpujune2011-313339.html

Failles

- Contournement DEP/ASLR
  - La JVM embarque MSVCR71.DLL qui est compilée sans aucune protection
    - http://www.whitephosphorus.org/sayonara.txt
  - Idem lorsque McAfee ou Symantec est installé …
    - http://www.scriptjunkie.us/2011/06/bypassing-dep-aslr-in-browser-exploits-with-mcafee-symantec/
- Mac OS X (2011-004)
  - 39 failles corrigées
    - ZDI-11-228, ZDI-11-229, ZDI-11-230, ZDI-11-231
    - http://support.apple.com/kb/HT4723
  - La mise à jour se passe mal
    - https://discussions.apple.com/message/15474962
- Jailbreakme.com
  - De nouveau opérationnel ☺
    - http://blog.iphone-dev.org/

Failles

- VMWare ESX
    - http://www.vmware.com/security/advisories/VMSA-2011-0009.html
- Qemu-kvm
  - Evasion de l'invité
    - http://rhn.redhat.com/errata/RHSA-2011-0919.html

- Symantec Web Gateway
  - ZDI-11-233: injection SQL dans "forget.php"

- HPOV Storage Data Protector
    - http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c02712867

Failles 2.0

- **Dropbox #fail**
  - http://blog.dropbox.com/?p=821
  - http://www.securityvibes.fr/marche-business/dropbox-faille-authentification/
- **Dropbox #fail (again)**
  - Changement du CLUF
- **Failles triviales sur le site developer.apple.com**
  - http://seclists.org/fulldisclosure/2011/Jul/3
- **Facebook lance l'alerte suicide**
  - http://www.20minutes.fr/article/683250/web-une-alerte-suicide-creee-facebook
- **Un outil de "*precrime*" sur Facebook**
  - Le produit Agatha
    - http://www.zataz.com/news/21349/espionnage--facebook.html
  - Notons que les militaires américains pratiquent déjà
    - http://www.rawstory.com/rs/2011/02/22/exclusive-militarys-persona-software-cost-millions-used-for-classified-social-media-activities/

Sites piratés

- Les sites piratés du mois
  - Mt. Gov
    - A provoqué le "crash" de la monnaie BitCoin
      - http://www.dailytech.com/Inside+the+MegaHack+of+Bitcoin+the+Full+Story/article21942.htm
  - CitiGroup (suite)
    - $2,7 millions ont été détournés
      - http://www.thestreet.com/story/11166596/1/citigroup-hackers-stole-27-million.html
    - … en changeant un ID dans l'URL
      - http://www.dailymail.co.uk/news/article-2003393/How-Citigroup-hackers-broke-door-using-banks-website.html
  - StartSSL
      - http://www.theregister.co.uk/2011/06/21/startssl_security_breach/
  - Le Ministère de la Défense français victime d'empoisonnement DNS
      - http://www.antispam.fr/fr/news/20110615.asp

Sites piratés

- **Le compte Twitter de Fox News**
    - http://www.alternet.org/newsandviews/article/629324/hackers_breach_fox_news_twitter_account,_tweet_fake_obama_death_notice/
- **Sega (Sega Pass)**
    - 1,29 million de comptes
        - http://www.securityvibes.fr/menaces-alertes/sega-piratage-data-breach/
- **Piratages, suites …**
    - OTAN
        - https://www.infosecisland.com/blogview/15035-Team-Inject0r-The-Multinational-Connection.html
    - FMI
        - http://www.newsfactor.com/news/Did-Foreign-Government-Hack-IMF-/story.xhtml?story_id=0310012HP9HP
    - Coût moyen d'un *databreach* selon Ponemon = $7,2 millions
        - http://www.symantec.com/content/en/us/about/media/pdfs/symantec_ponemon_data_breach_costs_report.pdf

Sites piratés

- Lulzsec
  - La base de données du recensement anglais piratée
    - http://www.telegraph.co.uk/technology/news/8589078/Hackers-steal-entire-2011-census.html
  - Le leader de Lulzsec identifié ?
    - http://www.liquidmatrix.org/blog/2011/06/25/lulzsec-leader-sabu-outed/
  - Ainsi que d'autres membres …
    - http://lulzsecexposed.blogspot.com/
    - http://www.guardian.co.uk/uk/2011/jun/21/hackers-lulzsec-arrest-essex-census
    - http://nakedsecurity.sophos.com/2011/06/30/lulzsec-suspect-hacking-search/
    - http://pastebin.com/5NJXfbVw
    - http://www.pastie.org/2173213
- A lire aussi
    - http://www.lemonde.fr/technologies/article/2011/06/24/lulzsec-l-ascension-eclair-d-un-groupe-de-pirates-informatiques_1540672_651865.html
- Fun
    - http://hassonybeenhackedthisweek.com/
- Bon
    - https://shouldichangemypassword.com/
- Pas bon
    - http://ismycreditcardstolen.com/

Malwares et spam

- TDL-4
  - Le botnet le plus gros et le plus résilient ?
    - http://www.lemondeinformatique.fr/actualites/lire-tdl-4-un-botnet-quasi-indestructible-a-fait-son-apparition-34100.html
    - http://www.computerworld.com/s/article/9218034/Massive_botnet_indestructible_say_researchers?taxonomyId=82&pageNumber=1

- Un outil de déni de service
  - Basé sur le réseau Tor
    - http://pastebin.com/raw.php?i=MLFs5m1K

- Tentative de déstabilisation de Mikko Hypponen et Brian Krebs
    - http://www.theregister.co.uk/2011/06/13/hack_punts_bogus_cybercrime_story/

- McAfee attaque les implants médicaux
  - Et recrute Barnaby Jack pour l'occasion
    - http://www.msnbc.msn.com/id/43443216/ns/technology_and_science-security/

- Les faux antivirus
  - Un marché juteux
    - http://www.securityvibes.fr/cyber-pouvoirs/faux-antivirus-marche-a-plusieurs-millions-deuros/

Actualité (francophone)

- "Droits de l'individu dans la révolution numérique"
  - http://www.assemblee-nationale.fr/13/rap-info/i3560.asp

- Certigna #fail
  - Note: ceci n'a aucun impact sur la sécurité de l'autorité
    - http://www.thinq.co.uk/2011/6/9/certigna-publishes-ssl-private-key-mistake/

Actualité (anglo-saxonne)

- Le projet "*shadow network*" poussé par Obama
  - Internet dans une valise
    - http://www.nytimes.com/2011/06/12/world/12internet.html?_r=3
    - http://www.youtube.com/watch?v=4kNEsw0Aj2U

- Mot de passe + question secrète = suffisant pour du e-banking
  - Les banques vont pouvoir arrêter de rembourser …
    - http://krebsonsecurity.com/2011/06/court-passwords-secret-questions-reasonable-ebanking-security/

Actualité (européenne)

- Vers une criminalisation européenne des outils offensifs ?
  - http://www.theregister.co.uk/2011/06/14/making_hacking_tools_should_be_criminal_act_say_eu_ministers/
- L'OCSE (Organization for Security and Cooperation in Europe) s'engage pour la cybersécurité
  - http://www.oscepa.org/images/stories/documents/activities/1.Annual%20Session/2011_Belgrade/Supplementary_Items/04_Overall_Approach_by_the_OSCE_to_Promote_Cybersecurity_Belgium_ENGLISH.pdf

Actualité (Google)

- Google lance Google+
  - Nouvelle tentative de réseau social

- Google "blackliste" tous les domaines ".cz.cc"
  - http://blog.sucuri.net/2011/06/google-blacklisted-all-the-cz-cc-domains.html

- C'est la fin pour Google Health et PowerMeter

- ChromeOS fondamentalement bogué ?
  - http://news.cnet.com/8301-1009_3-20075801-83/chrome-os-has-security-flaws-claims-researcher/

- SWF vers HTML5
  - http://swiffy.googlelabs.com/

Actualité (crypto)

- **John the Ripper propose une optimisation des S-Box DES**
  - **Gain de performance > 12%**
    - **http://www.openwall.com/lists/john-users/2011/06/22/1**
    - **http://it.slashdot.org/story/11/07/01/1734213/17-Smaller-DES-S-box-Circuits-Found**

- **TrueCrypt FAIL ?**
    - **http://16s.us/TCHunt/discrepancy/**

- **Exploitation des canaux cachés acoustiques**
    - **http://www.cs.tau.ac.il/~tromer/acoustic/**

Actualité

- **Sorties logicielles**
  - Metasploit 3.7.0
    - Support de la signature SMB
  - Metasploit 3.7.1
  - Metasploit 3.7.2
  - Vega Beta 1 (audit d'application Web)
    - http://keystream.subgraph.com/2011/07/01/vega-beta-release/

Actualité

- **Patriot Act vs. Sécurité du Cloud**
  - http://www.zdnet.com/blog/igeneration/microsoft-admits-patriot-act-can-access-eu-based-cloud-data/11225
- **Robert Morris est mort**
  - http://www.nytimes.com/2011/06/30/technology/30morris.html

Fun

- Fun list
  - http://infosuck.org/
  - http://dis.4chan.org/read/prog/1295544154
  - http://www.asciiflow.com/
  - http://spectrum.ieee.org/static/hacker-matrix
- Hacker … à partir de 8 ans ?
  - http://www.huffingtonpost.com/2011/06/24/defcon-kids-hacker-conference_n_883791.html
- Apple pas très fair-play
  - http://www.theregister.co.uk/2011/06/08/apple_copies_rejected_app/
- Il y a une application pour tout
  - http://delapubmaispasque.fr/2011/06/10/application-facebook-if-i-die-envoyer-un-message-apres-votre-mort/

Questions / réponses

- **Questions / réponses**

- **Prochaine réunion**
  - **Mardi 13 septembre 2011**

- **N'hésitez pas à proposer des sujets et des salles**