OSSIR
Groupe Paris

Réunion du 14 juin 2011

Revue des dernières vulnérabilités

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

Avis Microsoft

- **Juin 2011**
  - **16 bulletins, dont 9 critiques et 7 importants**
    - **34 failles**
  - **Produits affectés:**
    - **Microsoft Windows, Microsoft Office, Internet Explorer, .NET, SQL, Visual Studio, Silverlight, ISA**
  - **Un correctif contre le "cookie jacking" ?**
- **Advisories**
  - **Aucun**
- **Révisions**
  - **Aucune**

Infos Microsoft

- **Sorties logicielles**
  - **Office 2010 SP1 et SharePoint 2010 SP1 prévus pour fin juin**
  - **EMET 2.1**
    - **http://blogs.technet.com/b/srd/archive/2011/05/18/new-version-of-emet-is-now-available.aspx**
  - **Rappel: Vista SP1 est en fin de vie à partir du 12 juillet 2011**
    - **http://www.microsoft.com/windows/enterprise/products/windows-7/end-of-support.aspx**

Infos Microsoft

- **Autre**
  - **Microsoft Security Intelligence Report**
    - **Volume 10**
      - **http://www.microsoft.com/security/sir/default.aspx**
  - **Les 10 lois immuables de la sécurité … ont changé !**
    - **http://technet.microsoft.com/en-us/library/hh278941.aspx**
  - **Une faille corrigée dans Hotmail**
    - **http://www.theregister.co.uk/2011/05/24/microsoft_hotmail_email_theft_attack/**

Infos Réseau

- **(Principales) faille(s)**
  - **Cisco IOS-XR**
    - **Déni de service sur SSHv1**
      - **http://www.cisco.com/en/US/products/products_security_advisory09186a0080b7f18f.shtml**
  - **Cisco IOS-XR**
    - **Faille dans la pile IP, et autres**
      - **http://www.cisco.com/en/US/products/products_security_advisory09186a0080b7f18e.shtml**
      - **http://www.cisco.com/en/US/products/products_security_advisory09186a0080b7f191.shtml**
  - **Cisco RVS 4000**
      - **http://www.cisco.com/en/US/products/products_security_advisory09186a0080b7f190.shtml**
  - **Cisco Content Delivery Streamer**
      - **http://www.cisco.com/en/US/products/products_security_advisory09186a0080b7f18b.shtml**
  - **Cisco Media Experience Engine 5600**
    - **Compte "root" avec mot de passe par défaut**
      - **http://www.cisco.com/warp/public/707/cisco-sa-20110601-mxe.shtml**
  - **Cisco AnyConnect**
    - **Failles multiples**
      - **http://www.cisco.com/warp/public/707/cisco-sa-20110601-ac.shtml**
  - **Cisco Network Registrar**
    - **Compte par défaut**
      - **http://www.cisco.com/warp/public/707/cisco-sa-20110601-cnr.shtml**
  - **Cisco IP Phones 7900**
    - **Failles multiples**
      - **http://www.cisco.com/warp/public/707/cisco-sa-20110601-phone.shtml**

Infos Réseau

- **Autres infos**
  - **"IPv6 RA Guard Evasion" (draft)**
    - **http://tools.ietf.org/id/draft-gont-v6ops-ra-guard-evasion-00.txt**
  - **Le langage OPA devient un projet OWASP**
    - **Cf. SSTIC 2010**
      - **https://www.owasp.org/index.php/Opa#tab=Project_About**
      - **http://opalang.org/**

Infos Unix

- **(Principales) faille(s)**
  - **Bind**
    - **Déni de service (DNSSEC, encore …)**
      - **http://www.isc.org/software/bind/advisories/cve-2011-1910**
  - **Vino (VNC Server pour Gnome)**
    - **http://www.ubuntu.com/usn/usn-1128-1/**
  - **Dovecot < 2.0.13, < 1.2.17**
    - **Déni de service**
      - **http://dovecot.org/pipermail/dovecot//2011-May/059085.html**
      - **http://dovecot.org/pipermail/dovecot//2011-May/059086.html**
  - **Apache sur OS/400**
    - **Déni de service**
      - **http://www-01.ibm.com/support/docview.wss?uid=nas2be723d486f51dd5386257895003ca15c&wv=1**

Infos Unix

- Apache Tomcat < 7.0.14
  - Fuite d'informations
    - http://tomcat.apache.org/security-7.html
- Apache SVN
  - Principalement des dénis de service
    - http://subversion.apache.org/security/CVE-2011-1752-advisory.txt
    - http://subversion.apache.org/security/CVE-2011-1783-advisory.txt
    - http://subversion.apache.org/security/CVE-2011-1921-advisory.txt
- IBM WebSphere 6.x et 7.x
  - XSS
    - http://www.securelist.com/en/advisories/44700
- phpMyAdmin
  - XSS & Open Redirect
    - http://www.phpmyadmin.net/home_page/security/PMASA-2011-3.php
    - http://www.phpmyadmin.net/home_page/security/PMASA-2011-4.php
- Wordpress < 3.1.13
  - Failles multiples
    - http://wordpress.org/news/2011/05/wordpress-3-1-3/

Infos Unix

- Zope
  - Usurpation d'identité (triviale)
    - https://mail.zope.org/pipermail/zope-announce/2011-May/002257.html
- Plone
  - XSS et usurpation d'identité
    - http://plone.org/products/plone/security/advisories/CVE-2011-1948
    - http://plone.org/products/plone/security/advisories/CVE-2011-1949
    - http://plone.org/products/plone/security/advisories/CVE-2011-1950
- Ruby on Rails
  - Contournement du filtre anti-XSS
    - http://weblog.rubyonrails.org/2011/6/8/potential-xss-vulnerability-in-ruby-on-rails-applications
- Drupal
  - XSS
    - http://drupal.org/node/1168756
- Horde_Auth < 1.0.4
  - Contournement de l'authentification
    - http://lists.horde.org/archives/announce/2011/000638.html

Infos Unix

- Autre
  - Une proposition intéressante
    - Randomisation du kernel au boot
      - http://marc.info/?l=linux-kernel&m=130626913317973&w=2
  - SECCOMP filters
    - C'est mal parti …
      - http://article.gmane.org/gmane.linux.kernel/1145636

Failles

- **Principales applications**
  - **Chrome < 12.0.742.91**
    - **http://googlechromereleases.blogspot.com/2011/06/chrome-stable-release.html**
    - **Contrôle des téléchargements, effacement des LSO, accélération 3D, …**
      - **http://chrome.blogspot.com/2011/06/chrome-12-safer-and-snazzier.html**
  - **Opera < 11.11**
    - **http://www.opera.com/support/kb/view/992/**
  - **Flash < 10.3.181.22 / 10.3.181.23**
    - **Attaqué en "0day"**
      - **http://www.adobe.com/support/security/bulletins/apsb11-13.html**
  - **Oracle Quaterly Patch**
    - **Ne concerne que Java < 1.6.0_26**
    - **17 failles corrigées**
      - **http://www.oracle.com/technetwork/topics/security/javacpujune2011-313339.html**

Failles

- WireShark < 1.4.7, < 1.2.17
  - http://www.wireshark.org/security/wnpa-sec-2011-08.html
- VLC < 1.1.10
  - http://www.videolan.org/security/sa1104.html
- VMWare ESX & WorkStation
  - Failles multiples
    - http://www.vmware.com/security/advisories/VMSA-2011-0009.html
- IBM Tivoli
  - Compte par défaut (ZDI-11-169) et "buffer overflow" (256 octets …)
    - https://www-304.ibm.com/support/docview.wss?uid=swg21499146&wv=1
- Symantec BackupExec
  - Authentification insuffisante des agents
    - http://www.symantec.com/business/security_response/securityupdates/detail.jsp?fid=security_advisory&pvid=security_advisory&year=2011&suid=20110526_00
- Contrôleurs réseau Intel 82598 et 82599 (10Gbe)
  - Déni de service à distance
    - http://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00028&languageid=en-fr

Failles

- Lotus Notes
  - Failles multiples dans le traitement des pièces jointes
    - https://www-304.ibm.com/support/docview.wss?uid=swg21500034&wv=1

- Multiples produits Symantec
  - Mêmes failles que précédemment: ces failles sont dans la librairie Autonomy KeyView
    - http://www.symantec.com/business/security_response/securityupdates/detail.jsp?fid=security_advisory&pvid=security_advisory&year=2011&suid=20110531_00

Failles 2.0

- Comparaison des scanneurs de code source C/C++ et Java
  - Un projet NSA & OWASP
  - Aucun outil n'a trouvé plus de 15% des failles sans générer de faux positif
    - https://lists.owasp.org/pipermail/owasp-leaders/2011-May/005192.html
- Twitter #fail
    - http://serphacker.com/twitter/twitter-new-follow-button-clickjacking-attack.html
- LinkedIn #fail
    - http://www.wtfuzz.com/blogs/linkedin-ssl-cookie-vulnerability/
- Facebook devient un site de commerce social
  - Plus il y a d'argent, plus il y a d'attaques

Sites piratés

- **Les sites piratés du mois**
  - **Sony (plusieurs fois)**
    - **Ca devient vraiment difficile à suivre !**
      - **http://attrition.org/security/rants/sony_aka_sownage.html**
  - **TMG**
    - **http://pastebin.com/Rc1zGXu0**
    - **Note: TMG va être audité**
      - **http://www.hsc.fr/presse/communiques.html.fr#080611**
  - **Lockheed Martin**
    - **A travers ses tokens RSA**
      - **http://www.reuters.com/article/2011/05/26/lockheed-network-idUSN2613783420110526**
      - **http://www.reuters.com/article/2011/05/28/usa-defense-hackers-idUSN2717936920110528**
  - **Ainsi que L-3**
    - **http://www.wired.com/threatlevel/2011/05/l-3/**
  - **… car oui, les *seeds* RSA ont bien fuité !**
    - **RSA va remplacer 40 millions de tokens**
      - **http://arstechnica.com/security/news/2011/06/rsa-finally-comes-clean-securid-is-compromised.ars**

Sites piratés

- Le FMI
  - http://www.nytimes.com/2011/06/12/world/12imf.html?_r=2
- Comodo Brésil
  - Injection SQL simple
    - http://pastebin.com/F5nUf5kr
- Citigroup
  - 200,000 données bancaires volées
    - http://searchsecurity.techtarget.com/news/2240036729/Citigroup-acknowledges-data-security-breach
- LulzSec (!)
  - http://archives.neohapsis.com/archives/fulldisclosure/2011-06/0075.html
  - Pourtant ils s'y connaissent …
    - http://lulzsecurity.com/releases/
- Le meilleur reste à venir
  - OTAN vs. Anonymous
    - http://news.cnet.com/8301-1009_3-20070283-83/anonymous-warns-nato-not-to-challenge-it/

Sites piratés

- Le gouvernement iranien
  - http://www.theepochtimes.com/n2/world/anonymous-leaks-10000-e-mails-from-iranian-government-57143.html
- PBS
  - PBS = télévision publique américaine
    - http://pastebin.com/0YULt1ZG
- L'une des deux centrales électriques Lettones
  - http://seclists.org/fulldisclosure/2011/May/85

Malwares et spam

- Il y a désormais un antivirus officiel pour Mac OS X
  - Même s'il ne s'appelle pas "antivirus"
    - http://support.apple.com/kb/HT4657

- Une étude du EdelWeb + CLUSIF sur l'argent des pharmacies en ligne
    - http://blogs.mcafee.com/mcafee-labs/finding-the-money-behind-rogue-pharmacies

Actualité (francophone)

- Cyber-commandos, fondation de recherche privée …
  - L'ANSSI a des projets dans ses cartons !
    - http://www.lepoint.fr/high-tech-internet/la-france-cree-des-commandos-de-cyberdefense-26-05-2011-1335572_47.php
    - http://www.securityvibes.fr/cyber-pouvoirs/anssi-cyber-commandos/
  - Un projet déjà terminé: refaire le site Web ☺
- L'intranet de l'institut Mines-Telecom confié à Google
  - http://www.pcinpact.com/actu/news/63859-mines-telecom-extranet-intranet-google.htm
- Le projet Idénum est lancé
  - http://lexpansion.lexpress.fr/high-tech/des-nouvelles-du-projet-d-identifiant-numerique-universel_256413.html
- Quant l'agence de communication HADOPI dérape
  - http://reflets.info/le-pur-fail-agenceh-hadopi-eurorscg/
- Conférence SSTIC 2011
  - Cf. compte-rendu ce jour ☺

Actualité (anglo-saxonne)

- Le FBI se bat pour continuer à pouvoir espionner
  - … directement chez les ISP
    - http://www.theregister.co.uk/2011/05/12/fbi_protects_isps/

Actualité (européenne)

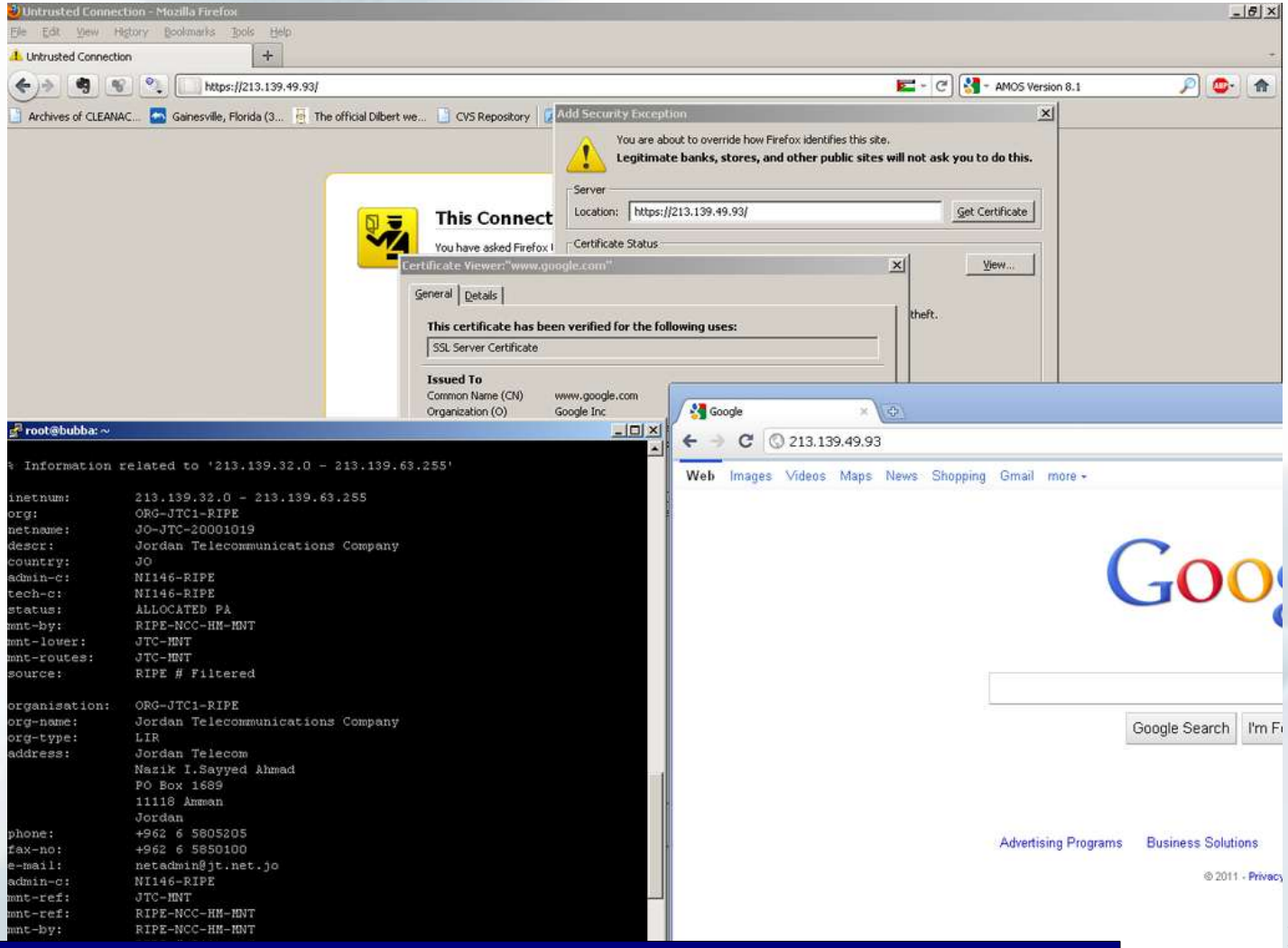
- Le pare-feu européen continue à faire des vagues
  - Projet "Virtual Schengen Border"
    - http://h16free.com/2011/05/16/8311-schengen-virtuel-danger-reel

Actualité (Google)

- Nombreuses annonces pour Google I/O
  - Google Wallet
    - http://www.google.com/wallet/how-it-works.html
  - Les principaux constructeurs de téléphones s'engage à fournir des mises à jour pendant 18 mois
  - …
- Google encore attaqué par la Chine ?
  - http://googleblog.blogspot.com/2011/06/ensuring-your-information-is-safe.html
- VUPEN vs. Chrome
  - Evasion de la sandbox … via un plugin
    - http://www.vupen.com/demos/VUPEN_Pwning_Chrome.php

Actualité (Google)

- Google en Jordanie … ou l'échec du SSL



Actualité (mobile)

- Un nouveau malware pour Android
  - Originalité: chargement dynamique de classes pour échapper à l'analyse statique de Google
    - http://www.csc.ncsu.edu/faculty/jiang/Plankton/
- FaceNiff
  - Le FireSheep pour Android
- Un nouveau projet OWASP dédié à la sécurité des mobiles
    - https://www.owasp.org/index.php?title=OWASP_Mobile_Security_Project_Call_For_Volunteers
- HTC
  - Verrouillera ou verrouillera pas ses ROM ?
    - http://www.androidcentral.com/htc-were-reviewing-our-bootloader-policy
- Les téléphones de Kate Middleton et Tony Blair piratés
    - http://www.guardian.co.uk/uk/2011/jun/08/phone-hacking-kate-middleton-tony-blair

Actualité (crypto)

- **Sérieux problème sur ECDSA**
  - **"Timing attack" sur l'implémentation OpenSSL**
    - **http://eprint.iacr.org/2011/232.pdf**

- **Les fichiers de Ben Laden "déchiffrés à 95%"**
  - **http://www.hindustantimes.com/Bin-Laden-computer-files-95-decrypted/Article1-707669.aspx**

- **Le chiffrement matériel de disque devient "*mainstream*"**
  - **http://www.trustedcomputinggroup.org/files/static_page_files/67318BEF-1A4B-B294-D00BDAD736433305/TCG_Ponemon_SED_Survey_Report.Final.pdf**

Actualité

- Sorties logicielles
  - Apple iOS 5 + Apple iCloud
    - Note: iOS 5 est déjà jailbreaké
      - http://www.theregister.co.uk/2011/06/07/ios_five_jailbroken/
  - Origami PDF 1.0
    - http://esec-lab.sogeti.com/dotclear/index.php?post/2011/05/24/Origami-1.0-released%21
  - Burp 1.4
    - http://blog.portswigger.net/2011/06/burp-suite-free-edition-v14-released.html
  - Un site collectant tous les supports de présentation en sécurité
    - http://cc.thinkst.com/

Actualité

- Skype entièrement "reversé"
  - Une implémentation Open Source disponible
  - … pendant quelques jours
    - http://skype-open-source.blogspot.com/2011/06/skype-protocol-reverse-engineered.html
    - http://www.ewdn.com/2011/06/05/ewdn-exclusive-an-interview-with-efim-bushmanov/
- La reconnaissance faciale sur Facebook fait débat
    - http://nakedsecurity.sophos.com/2011/06/07/facebook-privacy-settings-facial-recognition-enabled/
- Intel implémente une nouvelle protection
  - SMEP (*Supervisor Mode Execution Protection*)
    - http://theinvisiblethings.blogspot.com/2011/06/from-slides-to-silicon-in-3-years.html
- Une présentation sur une faille SCADA annulée
  - A la demande de Siemens et du gouvernement américain
    - http://news.infracritical.com/pipermail/scadasec/2011-May/019934.html
    - https://twitter.com/#!/SCADAhacker/status/71124494181347328

Fun

- Une clé USB "sécurisée"
  - http://www.likecool.com/Safest_USB--Design--Gear.html
- Ca n'était pas du vaporware
  - Duke Nukem Forever est sorti

Questions / réponses

- Questions / réponses
- Prochaine réunion
  - Mardi 12 juillet 2011
- N'hésitez pas à proposer des sujets et des salles