OSSIR
Groupe Paris

Réunion du 13 décembre 2011

Revue des dernières vulnérabilités

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

Avis Microsoft

- **Novembre 2011**
  - **4 bulletins, ??? failles**
  - **MS11-083 Faille dans la pile TCP/IP [2]**
    - **Affecte: Windows Vista / 2008 / Seven / 2008R2**
    - **Exploit:**
      - **Exploitation à distance sur un port UDP fermé**
        - **La faille qui tue …**
    - **Crédit: n/a**

Avis Microsoft

- MS11-084 Faille dans le support des polices TrueType
  - Affecte: Windows Seven / 2008R2
  - Exploit: déni de service à l'ouverture d'une police malformée
    - Exploitable à distance via IE et/ou WebDAV
  - Crédit: Will Dorman / CERT-CC

- MS11-085 "DLL Preloading" dans Windows Mail et Windows Meeting Space [1]
  - Affecte: Windows Vista / 2008 / Seven / 2008R2
  - Exploit: "DLL Preloading" à l'ouverture d'un fichier ".eml" ou ".wcinv"
  - Crédit: Ivan Sanchez / EvilCode

Avis Microsoft

- **MS11-086 Elévation de privilèges dans Active Directory [1]**
  - **Affecte: Windows (toutes versions supportées)**
  - **Exploit: un certificat révoqué peut être utilisé pour l'accès LDAP/SSL**
  - **Crédit: Xavier Lassoie & Sébastien Godard / Autosécurité**

Avis Microsoft

- **Prévisions pour Décembre 2011**
  - **14 bulletins, 20 failles**
  - **Corrigera probablement DuQu et BEAST**

- **Advisories**

  - **Q2269637 "DLL Preloading"**
    - **V12.0: ajout du bulletin MS11-085**

  - **Q2639658**
    - **V1.3: révision du workaround**
    - **V1.4: révision du workaround**

  - **Q2641690 Certificats SSL frauduleux (clé RSA-512 factorisée)**
    - **V1.0: avis initial**
    - **V2.0: re-publication de la mise à jour**

Avis Microsoft

- **Révisions**
  - **MS11-025**
    - **V4.1: correction des paramètres de ligne de commande du correctif**
  - **MS11-028**
    - **V2.4: corrections documentaires (Windows 7 SP1 et 2008R2 SP1)**
  - **MS11-037**
    - **V2.0: re-publication de la mise à jour pour Windows XP et 2003**
    - **V2.1: corrections documentaires**
  - **MS11-071**
    - **V2.0: mise à jour disponible pour Windows 7 Embedded**

Infos Microsoft

- **Sorties logicielles**
  - **Microsoft TellMe**
    - **L'alternative à Apple Siri**
      - **http://www.microsoft.com/en-us/tellme/**

Infos Microsoft

- Autre
  - MS11-071 laisse potentiellement une faille de sécurité
    - http://seclists.org/fulldisclosure/2011/Nov/244
  - Windows 8
    - Le "secure boot" contourné ?
      - http://www.pcpro.co.uk/news/security/371290/hacker-breaks-windows-8-secure-boot
    - Changement de stratégie sur Windows Update
      - http://blogs.msdn.com/b/b8/archive/2011/11/14/minimizing-restarts-after-automatic-updating-in-windows-update.aspx
    - Une bêta publique en février 2012 ?
      - http://www.linformaticien.com/actualites/id/22458/windows-8-beta-publique-en-fevrier.aspx
    - Un échec probable, selon IDC
      - http://www.solutions-logiciels.com/actualites.php?actu=10705

Infos Microsoft

- Microsoft Office … sur iPad
  - En 2012
    - http://www.linformaticien.com/actualites/id/22425/microsoft-office-arrive-sur-ipad-en-2012.aspx
- Windows Phone 7 … sur Android et iPhone
    - http://aka.ms/wpdemo
- Microsoft + Yahoo! + AOL vs. Google Ads
    - http://www.linformaticien.com/actualites/id/22175/microsoft-yahoo-et-aol-s-associent-dans-la-publicite.aspx
- Microsoft prépare son réseau social
  - Socl.com
    - http://www.theverge.com/2011/11/15/2517610/microsoft-socl-inside-the-companys-secret-social-network
- L'anniversaire de Windows XP
    - http://windowsteamblog.com/windows/b/business/archive/2011/10/25/commemorating-windows.aspx

Infos Microsoft

- SilverLight menacé ?
  - http://www.linformaticien.com/actualites/id/22196/la-fin-de-silverlight.aspx
- Bill Gates de retour chez Microsoft ?
  - http://www.linformaticien.com/actualites/id/22629/bill-gates-pourrait-reprendre-les-renes-de-microsoft.aspx

Infos Réseau

- (Principales) faille(s)
  - n/a

Infos Réseau

- **Autres infos**
  - **Un appel d'offres pour remplacer l'ICANN**
    - **Contrat de 3 ans**
    - **Le service doit être fourni gratuitement**
    - **Les soumissionnaires doivent être américains**
      - **http://www.lemonde.fr/technologies/article/2011/11/14/la-racine-du-net-soumise-a-un-appel-d-offres_1603342_651865.html**
  - **Le ".xxx" est ouvert**
    - **Compter $60 par nom …**
  - **RFC 6441: toutes les adresses IPv4 sont désormais allouées**
    - **http://www.bortzmeyer.org/6441.html**
  - **La surveillance d'Internet arrive aussi en Russie**
    - **http://securityaffairs.co/wordpress/?p=156**
    - **http://zakupki.gov.ru/pgz/public/action/orders/info/common_info/show?notificationId=258425**

Infos Réseau

- **Panne de DNS chez MegaUpload**
  - **http://www.linformaticien.com/actualites/id/22390/megaupload-est-presque-inaccessible.aspx**
- **Panne chez Level3**
  - **https://twitter.com/?photo_id=1#!/RafikSmati/status/138921918471471104/photo/1**

Infos Unix

- (Principales) faille(s)
  - Faille dans la glibc - fonction crypt()
    - Utilisation de alloca() sans limitation
      - http://www.openwall.com/lists/oss-security/2011/11/15/1
  - Le compte "Guest" dans Ubuntu fait débat
    - https://answers.launchpad.net/ubuntu/+source/lightdm/+question/175756
  - Linux: "buffer overflow" avec un nom de fichier trop long …
    - … sur un système HFS
      - http://git.kernel.org/?p=linux/kernel/git/torvalds/linux.git;a=commit;h=bc5b8a9003132ae44559edd63a1623b7b99dfb68
    - Remonté par NetASQ ☺
  - Linux: "heap overflow" dans le support X25
    - http://permalink.gmane.org/gmane.linux.network/207657

Infos Unix

- **Autre**
  - **Fin de support pout Debian 5**
    - **Le 6 février 2012**
  - **Le noyau 2.6.38+ consomme 35% en plus**
    - **A cause d'un bogue du support ASPM dans la plupart des BIOS**
    - **Pas de correctif attendu avant Linux 3.3**
      - **http://www.pcinpact.com/news/67040-linux-noyau-correction-probleme-surconsommation.htm**

Failles

- **Principales applications**
  - **"0day" en circulation**
    - **Adobe Reader (utilisé dans une attaque contre ManTech Corp.)**
      - **http://contagiodump.blogspot.com/2011/12/adobe-zero-day-cve-2011-2462.html**
    - **Flash Player (à vendre !)**
      - **http://archives.neohapsis.com/archives/dailydave/2011-q4/0081.html**
  - **FireFox < 3.6.24**
    - **http://www.mozilla.org/security/known-vulnerabilities/firefox36.html#firefox3.6.24**
  - **FireFox < 8.0**
    - **http://www.mozilla.org/security/known-vulnerabilities/firefox.html#firefox8**
  - **ThunderBird < 8.0**
    - **http://www.mozilla.org/security/known-vulnerabilities/thunderbird.html#thunderbird8**

Failles 2.0

- SCADA
  - La pompe n'a pas été piratée par des Russes
  - … mais le responsable était en vacances en Russie avec son BlackBerry
    - http://www.wired.com/threatlevel/2011/11/water-pump-hack-mystery-solved/
  - "Hall of Shame"
    - http://www.digitalbond.com/scadapedia/vulnerability-notes/insecure-products-list/
  - Exemple: "cette faille ne sera pas patchée"
    - http://www.digitalbond.com/2011/11/08/advantech-webaccess-first-on-insecure-products-list/
  - 17 "backdoors" dans le même PLC
    - Utilisé au CERN dans le LHC …
      - http://reversemode.com/index.php?option=com_content&task=view&id=80&Itemid=1

Failles 2.0

- CarrierIQ
  - Faits
    - La plupart des téléphones commercialisés aux USA sont équipés d'un "outil de support"
      - http://androidsecuritytest.com/features/logs-and-services/loggers/carrieriq/
      - http://www.geek.com/articles/mobile/security-researcher-responds-to-carrieriq-with-video-proof-20111129/
      - http://vulnfactory.org/blog/2011/12/05/carrieriq-the-real-story/
  - Conséquences
    - Menaces sur le chercheur
      - http://www.h-online.com/security/news/item/Carrier-IQ-drops-cease-and-desist-against-security-researcher-1384209.html
    - Défausse sur les fabricants
      - http://www.h-online.com/security/news/item/Carrier-IQ-points-at-manufacturers-for-insecure-logs-1390359.html
  - Une seule chose à faire
      - http://www.extremetech.com/computing/107427-carrier-iq-which-phones-are-infected-and-how-to-remove-it

Failles 2.0

- **Imprimantes HP**
  - **Faits**
    - **http://redtape.msnbc.msn.com/_news/2011/11/29/9076395-exclusive-millions-of-printers-open-to-devastating-hack-attack-researchers-say**
    - **Peuvent être reprogrammées par une simple impression**
      - **Pas de signature du firmware**
    - **Sécurités désactivées ⇨ incendie possible**
  - **Conséquences**
    - **Action collective contre HP (une première)**
      - **http://docs.justia.com/cases/federal/district-courts/california/candce/5:2011cv05779/248220/1/0.pdf**

Failles 2.0

- Comment pirater le "Cloud" ?
  - Avec Google Search !
    - http://www.stachliu.com/slides/2011/Hacker%20Halted%202011%20-%20Pulp%20Google%20Hacking%20-%2027Oct2011.pdf
- Download.com ajoute son "badware"
    - http://seclists.org/nmap-hackers/2011/5
- Des TPE de supermarché piratés
    - http://arstechnica.com/business/news/2011/12/hackers-hit-supermarket-self-checkout-lanes-steal-money-from-shoppers.ars

Failles 2.0

- Facebook bientôt en bourse ?
  - Valorisé autour de $100 milliards …
    - http://www.linformaticien.com/actualites/id/22398/facebook-preparerait-son-ipo.aspx
- Faille(s) dans Facebook
  - Saturé par des images "porno" ☺
    - http://zataz.com/news/21726/image--porno--facebook--datasecuritybreach.fr.html
  - Les utilisateurs copient/collent du JavaScript sans comprendre
    - http://research.zscaler.com/2011/11/facebook-anatomy-of-self-inflicted.html?mid=53186
  - Il était possible de voir les photos de n'importe qui …

Failles 2.0

Sites piratés

- Les sites piratés du mois
  - Gemnet (autorité de certification Néerlandaise)
    - Via un PhpMyAdmin sans mot de passe …
      - http://paulsparrows.wordpress.com/2011/12/10/another-certification-authority-breached-the-12th/
  - Steam
    - http://store.steampowered.com/news/6761/
  - Le GSM à Gaza
    - http://www.infosecurity-magazine.com/view/21794/hackers-down-landline-and-cellular-systems-in-gaza-and-west-bank/
  - Plusieurs pompes à eau dans l'Illinois
    - De manière assez triviale …
      - http://pastebin.com/Wx90LLum

Sites piratés

- Les bases de données de l'UMP
  - … de manière assez triviale
    - http://www.linformaticien.com/actualites/id/22161/piratage-ump-une-operation-salutaire.aspx
- BFM TV
  - Pour "dénoncer les Anonymous et protéger les infrastructures critiques" (?!)
    - http://www.linformaticien.com/actualites/id/22187/bfm-tv-pirate-pour-denoncer-les-anonymous.aspx
- Orange.mg
  - Au travers d'une injection SQL
    - Dans le cadre de l'opération "OrangeStorm" …
  - Portail basé sur Joomla!
    - http://www.undernews.fr/alertes-securite/orange-madagascar-victime-dune-grosse-faille-de-securite.html

Sites piratés

- L'ONU
  - http://thehackernews.com/2011/11/oprobinhood-thousands-of-united-nation.html
- Le centre de calcul national indien
  - http://ictps.blogspot.com/2011/11/indias-national-informatics-centre.html
- Allezdax.com
  - Les pirates ont confondu avec la bourse allemande (DAX)
    - http://www.theregister.co.uk/2011/11/04/french_rugby_site_hacktivist_maul/

Malwares et spam

- De nombreuses entreprises infectées par des malwares inconnus
  - Attention: c'est un "pitch" de Palo Alto Networks
    - http://www.net-security.org/malware_news.php?id=1904
- Des certificats RSA-512 du gouvernement malaysien utilisés pour signer des malwares …
  - La clé a probablement été factorisée
    - http://blog.fox-it.com/2011/11/21/rsa-512-certificates-abused-in-the-wild/
    - http://www.f-secure.com/weblog/archives/00002269.html

Actualité (francophone)

- http://www.data.gouv.fr/
- Une loi contre la divulgation d'informations industrielles
  - Quel(s) objectif(s) ?
    - http://www.lesechos.fr/journal20111114/lec2_industrie/0201735283194-espionnage-industriel-une-nouvelle-loi-en-vue-pour-mieux-proteger-les-entreprises-248287.php
- Création d'une communauté française autour du forensics Open Source
    - http://blog.crimenumerique.fr/2011/12/08/lancement-dune-communaute-opensource-pour-linvestigation-numerique/
- Formation conjointe Telecom Paris/ANSSI
    - http://www.infodsi.com/articles/125388/telecom-sudparis-renforce-formation-experts-securite.html

Actualité (francophone)

- Après les disques durs, la SACEM envisage de taxer le Cloud …
  - http://www.linformaticien.com/actualites/id/22454/la-sacem-songe-a-la-taxation-du-cloud-computing.aspx
- HADOPI 3 vs. Streaming
  - http://www.ecrans.fr/Sarkozy-fait-chanter-les,13564.html
- Assignation des FAI contre le streaming
  - Quelles conséquences potentielles ?
    - http://www.linformaticien.com/actualites/id/22430/streaming-les-lobbies-du-cinema-assignent-les-fai.aspx
- Déploiement de la fibre optique en France
  - Il faudrait 180 ans au rythme actuel …
    - http://www.linformaticien.com/actualites/id/22453/le-tres-haut-debit-a-toute-petite-vitesse.aspx
- RueDuCommerce récupère 1 million d'euros chez Copie France
  - http://www.pcinpact.com/news/67426-copie-france-privee-jugement-rueducommerce.htm

Actualité (anglo-saxonne)

- Le NIST publie SAMATE 4.0
  - Software Assurance Metrics and Tool Evaluation
    - http://www.infosecurity-magazine.com/view/22201/nist-expands-database-designed-to-help-programers-improve-software-security/
- Le DHS n'aime pas les hackers
  - … et fait tout pour les ennuyer
    - http://www.theregister.co.uk/2010/11/19/dhs_detains_hacker/
- Un satellite de la NASA "hijacké" par les Chinois
  - En 2007 et en 2008
    - http://www.geek.com/articles/geek-pick/chinese-hackers-took-control-of-nasa-satellite-for-11-minutes-20111119/
- Le gouvernement anglais fait son propre "Challenge SSTIC"
    - http://www.canyoucrackit.co.uk/
    - http://twitpic.com/7han9l
  - Avec une vraie faille dedans ☺
    - https://twitter.com/#!/crypt0ad/status/142327735715495936/photo/1

Actualité (européenne)

- Le filtrage d'Internet est illégal en Europe
  - http://www.laquadrature.net/en/eu-court-of-justice-censorship-in-name-of-copyright-violates-fundamental-rights
- Google en abus de position dominante
  - Sur le choix des résultats dans la première page de recherche, par exemple
    - http://www.linformaticien.com/actualites/id/22447/antitrust-l-union-europeenne-tacle-google.aspx
- ENISA: les CERT ne font pas leur boulot
  - Pas de partage d'informations
  - Pas de proactivité
    - http://v3.co.uk/v3-uk/news/2131114/enisa-warns-certs-failing-sharing-proactive-threat-detection
- ENISA + OWASP
  - "Smartphone Secure Development Guidelines"
    - http://www.enisa.europa.eu/act/application-security/smartphone-security-1/smartphone-secure-development-guidelines

Actualité (Google)

- Android 4.0 "Ice Cream Sandwich" disponible
  - http://developer.android.com/index.html
- Google soutiendra juridiquement tous ses "partenaires" dans la téléphonie mobile
  - http://www.linformaticien.com/actualites/id/22165/google-annonce-qu-il-soutiendra-juridiquement-ses-partenaires.aspx
- Pas de clients pour les ChromeBooks
  - http://www.linformaticien.com/actualites/id/22173/les-chromebooks-se-vendent-mal.aspx
- Logitech abandonne GoogleTV
  - Mais LG pourrait s'y intéresser
    - http://www.linformaticien.com/actualites/id/22204/logitech-abandonne-google-tv-alors-que-lg-s-y-interesse.aspx
- N'oubliez pas de mettre "_nomap" dans votre SSID ☺
  - http://googlepolicyeurope.blogspot.com/2011/11/greater-choice-for-wireless-access.html

Actualité (Google)

- **Inauguration des locaux Google à Paris**
  - **http://googleblog.blogspot.com/2011/12/inaugurating-our-new-french.html**
  - **http://www.pcinpact.com/news/67461-nicolas-sarkozy-google-visite-questions-live.htm**

- **Google spécialiste de l'évasion fiscale**
  - **http://owni.fr/2011/04/19/google-irlande-bermudes-evasion-fiscale/**

Actualité (Apple)

- 3 ans pour corriger une faille dans les mises à jour iTunes
  - … utilisée par de nombreux "chevaux de Troie" gouvernementaux
    - http://krebsonsecurity.com/2011/11/apple-took-3-years-to-fix-finfisher-trojan-hole/
- Siri entièrement analysé
  - … par des français ☺
    - https://github.com/applidium/Cracking-Siri
- iTunes Match
  - Stockage de musique "dans le Cloud"
  - Disponible seulement aux USA
  - Pour $25/an

Actualité (crypto)

- La factorisation RSA-512 pour tous
  - https://github.com/GDSSecurity/cloud-and-control/tree/master/gnfs-info
- Le manuscrit du Copiale déchiffré
  - http://www.lefigaro.fr/hightech/2011/10/27/01007-20111027ARTFIG00593-le-secret-d-un-manuscrit-du-18e-siecle-a-ete-perce.php

Actualité

- Conférences
  - Passées
    - C&ESAR 2011
  - A venir
    - Hackito Ergo Sum
      - http://2012.hackitoergosum.org/cfp.txt
    - FrHACK
      - http://www.frhack.org/frhack-cfp.php
    - INFILTRATE
      - http://infiltratecon.com/speakers.html

- Sorties logicielles
  - GPG pour GMail
    - http://gpg4browsers.recurity.com/
  - "Reverse engineering" sous Mac OS X
    - http://bsr43.free.fr/Hopper/Home.html

Actualité

- L'escalade des nouveaux processeurs
  - Intel
    - 6 cœurs
  - AMD
    - 16 cœurs
      - http://www.linformaticien.com/actualites/id/22192/amd-et-intel-presentent-de-nouveaux-processeurs.aspx
  - ARM
    - GPU à 8 cœurs
      - http://www.linformaticien.com/actualites/id/22164/arm-devoile-un-processeur-pour-jouer-sur-smartphone-comme-sur-une-ps3.aspx
- Les salaires vont augmenter en 2012 !
  - http://www.bankinfosecurity.com/articles.php?art_id=4245

Actualité

- Les sociétés fournissant de la "cyber surveillance"
  - D'après WikiLeaks
    - http://wikileaks.org/the-spyfiles.html

- La "cyber surveillance"
  - Un marché évalué à $5 milliards
    - http://online.wsj.com/article/SB10001424052970203611404577044192607407780.html

Actualité

- Le BlackBerry aussi sera NFC
  - http://docs.blackberry.com/fr-fr/smartphone_users/deliverables/32554/CX_NFC_61_1524017_11.jsp
- RIM #fail
  - Ne pourra plus utiliser la marque "BBX"
    - http://www.v3.co.uk/v3-uk/news/2130712/rim-forced-rename-bbx-platform-blackberry-losing-legal-battle
- L'Inde se prépare à la "cyber offense"
  - http://articles.economictimes.indiatimes.com/2011-12-03/news/30471838_1_cyber-attacks-hackers-symantec-india
- webOS "bientôt" Open Source
  - http://www.hp.com/hpinfo/newsroom/press/2011/111209xa.html

Actualité

- Il n'y aurait que 12 équipes de pirates en Chine
  - http://news.smh.com.au/breaking-news-technology/a-few-hacker-teams-do-most-chinabased-data-theft-20111212-1or4l.html
- L'organisation de la "cyber reconnaissance" en Chine
  - http://project2049.net/documents/pla_third_department_sigint_cyber_stokes_lin_hsiao.pdf
- Huawei rachète sa Joint Venture avec Symantec
  - http://www.reuters.com/article/2011/11/14/us-huawei-symantec-idUSTRE7AD27520111114

Divers

- Décès de Paulo Pinto, alias CrashFR
  - http://www.hackerzvoice.net/node/155
- Le code source de Doom publié
  - https://github.com/TTimo/doom3.gpl
- BicaVM: une JVM en JavaScript
  - https://github.com/nurv/BicaVM
- Fortify 3.20 - 360 Server - Release Notes
  - Votre mot de passe ne peut pas contenir un "B"
    - https://twitter.com/#!/Foundstone/status/141544262620819458

Divers

- Hmmm …
  - (Attention, il est nécessaire de créer un compte pour avoir les résultats)
    - http://www.letudiant.fr/test/orientation/metier/etes-vous-fait-pour-devenir-informaticien.html
- Modifications de Wikipedia / seconde / pays
  - Entre 200 et 600 (!)
    - http://wikipulse.herokuapp.com/
- Autolib' est sous Windows
    - https://twitter.com/#!/Argusauto/status/143704961287593984/photo/1
- L'ordinateur du futur ?
    - http://www.fxitech.com/products/?mid=533
- telnet miku.acm.uiuc.edu

Questions / réponses

- Questions / réponses
- Prochaine réunion et assemblée générale annuelle
  - Mardi 10 janvier 2012
- N'hésitez pas à proposer des sujets