OSSIR
Groupe Paris

Réunion du 10 juillet 2012

Revue des dernières vulnérabilités

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

Avis Microsoft

- **Juin 2012**

  - **MS12-036 Faille dans RDP [1]**
    - **Affecte: Windows (toutes versions supportées)**
    - **Exploit: exécution de code à distance avant authentification**
    - **Crédit: n/d**

  - **MS12-037 Correctif cumulatif pour IE (x13) [1]**
    - **Affecte: Internet Explorer (toutes versions supportées)**
    - **Exploit:**
      - **Exécution de code (corruption mémoire)**
      - **Fuite d'information**
      - **Contournement des filtres**

Avis Microsoft

- **Crédit:**
  - **Anonymous + iDefense**
  - **Adi Cohen / IBM Security Systems**
  - **Roman Shafigullin / LinkedIn**
  - **Code Audit Labs / VulnHunt**
  - **Dark Son / VulnHunt**
  - **Qihoo 360 Security Center**
  - **Yichong Lin / McAfee Labs**
  - **Google Inc.**
  - **VUPEN Security + ZDI**
  - **Anonymous + ZDI (x5)**

Avis Microsoft

- MS12-038 Faille .NET Framework [1]
  - Affecte: .NET Framework (toutes versions supportées)
    - Sauf: .NET 1.0 SP3, 1.1 SP1, 3.0 SP2, 3.5 SP1
  - Exploit: évasion de la *sandbox*
    - http://weblog.ikvm.net/CommentView.aspx?guid=10e37c9a-593f-4ff1-bb2c-6f8a152cd8ac
  - Crédit: Vitaliy Toropov + ZDI

Avis Microsoft

- **MS12-039 Failles dans Lync (x4) [1]**
  - **Affecte:**
    - **Communicator 2007R2 (fuite d'information)**
    - **Lync 2010 (exécution de code à distance)**
  - **Exploit:**
    - **Exécution de code à l'ouverture d'un fichier .TTF malformé (x2)**
    - **"DLL Preloading"**
    - **Contournement du filtre HTML**
  - **Crédit:**
    - **hamburgers maccoy + Secunia SVCRP**
    - **Adi Cohen / IBM Security Systems**
    - **Alin Rad Pop + ZDI**

Avis Microsoft

- **MS12-040 Faille dans Microsoft Dynamics AX [1]**
  - **Affecte: Microsoft Dynamics AX 2012**
  - **Exploit: XSS**
  - **Crédit: Finian Mackin**

- **MS12-041 Failles noyau (x5) [1]**
  - **Affecte: Windows (toutes versions supportées)**
  - **Exploit: élévation de privilèges locale**
    - **Failles dans le support des Atoms (x3) - cf. Recon 2012**
    - **Faille dans le compteur de références sur les polices**
    - **Race condition dans WIN32K.SYS**
  - **Crédit:**
    - **Tarjei Mandt / Azimuth Security**
    - **Mateusz "j00ru" Jurczyk / Google Inc.**

Avis Microsoft

- MS12-042 Failles noyau (x2) [1]
  - Affecte:
    - Windows XP SP3 (x86)
    - Windows 2003 SP2 (x86)
    - Windows Seven "Gold" et SP1 (x64)
    - Windows 2008R2 "Gold" et SP1 (x64)
  - Exploit: élévation de privilèges locale
    - … en lien avec l'erreur de documentation Intel x64 (vs. AMD)
    - Faille dans "User Mode Scheduler"
    - Faille dans le support BIOS ROM
  - Crédit:
    - Rafal Wojtczuk / Bromium
    - Jan Beulich / SUSE

Avis Microsoft

- Advisories
  - Q2269637 DLL Preloading
    - V16.0: ajout du bulletin MS12-039
  - Q2718704 Certificat racine abusé par Flamer
    - V1.1: Windows Mobile et Windows Phone ne sont pas affectés
  - Q2719615 Faille dans MSXML exploitée "dans la nature"
    - V1.0: publication de l'avis
- Failles antérieures
  - MS11-087
    - http://www.f13-labs.net/news.html
- Failles à venir
  - ASP.NET "Partial Trust" n'a aucun sens
    - http://weblog.ikvm.net/CommentView.aspx?guid=509710e7-e9ce-4cf4-b7ed-130409a63161

Avis Microsoft

- **Prévisions pour Juillet 2012**
  - 9 bulletins, 16 failles
  - 3 critiques, 6 importants
  - Windows (x6), Office, SharePoint, Groove, Office Web Apps, VBA, …

- **Révisions**
  - M12-020
    - V2.0: réapplication du correctif pour Windows 7 et 2008R2
  - MS12-025
    - V2.0: réapplication du correctif
  - MS12-029
    - V1.2: mise à jour de la FAQ
  - MS12-034
    - V1.3: mise à jour de la FAQ
  - MS12-036
    - V1.1: ajout d'un *workaround* (utilisation du protocole NLA)

Infos Microsoft

- **Sorties logicielles**
  - **Les gammes Windows Server simplifiées**
    - **http://www.microsoft.com/en-us/server-cloud/windows-server/2012-editions.aspx**
    - **Windows Home Server disparait**
    - **Windows SBS disparait aussi**
  - **Patch bloquant les clés RSA < 1024 bits**
    - **Prévu pour diffusion en août 2012**
    - **Exception: les logiciels signés avant le 1er janvier 2010**
      - **http://blogs.technet.com/b/pki/archive/2012/06/12/rsa-keys-under-1024-bits-are-blocked.aspx**
  - **Windows Phone 8 présenté aux développeurs**
    - **http://www.zdnet.com/blog/microsoft/microsofts-windows-phone-8-theres-good-news-and-bad-news/12977**
    - **Se rapproche de Windows 8**
    - **Très orienté entreprises**
    - **Les terminaux actuels ne seront pas compatibles**
      - **Une version 7.8 sera présentée**
  - **Microsoft RMS pour Android**
    - **http://blogs.technet.com/b/rms/archive/2012/06/29/touchdown.aspx**

Infos Microsoft

- Autre
  - Les finalistes du "BlueHat Prize" annoncés
    - … tous ont proposé des techniques anti-ROP
    - 20 soumissions reçues
      - http://blogs.technet.com/b/ecostrat/archive/2012/06/21/bluehat-prize-v1.0-finalists.aspx
  - Skype installé automatiquement via WindowsUpdate
    - C'est un bug ☺
      - http://www.h-online.com/security/news/item/Microsoft-installs-Skype-without-consent-1627601.html
  - Microsoft infiltré par la NSA ?
    - http://www.itworld.com/security/281553/researcher-warns-stuxnet-flame-show-microsoft-may-have-been-infiltrated-nsa-cia
  - Un site de vente en ligne "taxe" les utilisateurs d'IE7
    - http://www.lifehacker.com.au/2012/06/kogan-imposing-tax-on-shoppers-who-use-ie7/
  - Un NAS de 32 To entièrement SSD
    - http://www.linformaticien.com/actualites/id/25203/microsoft-presente-un-nas-entierement-equipe-de-memoire-flash.aspx

Infos Microsoft

- La migration Windows XP vers Windows 8 coûtera 39€
- HP annonce la "HP Slate 8" sous x86
- Surface (demo) #fail ☺
  - http://www.journaldugeek.com/2012/06/20/surface-fail/
- Vanity Fair vs. Steve Ballmer
  - http://www.vanityfair.com/online/daily/2012/07/microsoft-downfall-emails-steve-ballmer
- Windows 8 sera-t-il un échec ?
  - http://betanews.com/2012/07/05/windows-8-will-flop/
- Microsoft va-t-il fabriquer son propre téléphone ?
  - http://www.businessinsider.com/microsoft-is-working-on-building-its-own-phone-says-nomura-2012-6
- "Microsoft Is the Most Exciting Company in Tech"
  - http://gizmodo.com/5889659/microsoft-is-the-most-exciting-company-in-tech-hands-down

Infos Microsoft

- Microsoft lance "le cimetière Google"
  - http://pinterest.com/googlegraveyard/google-graveyard/
  - Google lance la "morgue Microsoft"
    - http://pinterest.com/harrymccracken/microsoft-morgue/
- 30 personnes licenciées dans la division "publicité & Internet" de Microsoft France
  - En cause: "la position hégémonique d'un concurrent" …
    - http://www.linformaticien.com/actualites/id/25462/mini-plan-social-chez-microsoft-france.aspx
- Contrôle fiscal au siège de Microsoft France
  - http://www.linformaticien.com/actualites/id/25442/controle-fiscal-au-siege-de-microsoft-france.aspx
- Le siège de Microsoft en Grèce attaqué à l'explosif
  - http://www.linformaticien.com/actualites/id/25417/grece-le-siege-de-microsoft-attaque-avec-fusils-et-explosifs.aspx

Infos Réseau

- (Principales) faille(s)
  - Panne du réseau mobile Orange
    - Pendant plus de 10h …
  - Panne du *reverse DNS* du RIPE
    - "14:00 Discovery that backups are not available"
      - https://labs.ripe.net/Members/dfk/timeline-of-reverse-dns-events
  - Déni de service dans BIND
      - http://www.isc.org/software/bind/advisories/cve-2012-1667
  - Backdoor dans le routeur TP-Link WR740 (et d'autres)
      - http://www.websec.ca/advisories/view/root-shell-tplink-wdr740
    - Exploit
      - /userRpmNatDebugRpm26525557/linux_cmdline.html
      - User:osteam
      - Password:5up

Infos Réseau

- **Autres infos**
  - **RFC "Autonomous Internet"**
    - **Poussé par China Mobile**
      - **https://tools.ietf.org/html/draft-diao-aip-dns-00**
  - **La liste des candidats à un gTLD publiée**
    - **http://newgtlds.icann.org/en/program-status/application-results/strings-1200utc-13jun12-en**
  - **Ouverture des IDN le 3 juillet**
    - **http://www.afnic.fr/fr/l-afnic-en-bref/actualites/actualites-operationnelles/6104/showOperational/rappel-ouverture-aux-idn-demain-a-14h.html**
  - **L'ICANN conserve sont rôle**
    - **http://www.ntia.doc.gov/press-release/2012/commerce-department-awards-contract-management-key-internet-functions-icann**
  - **L'AFNIC conserve la gestion du ".fr" pour 5 ans**
    - **http://www.linformaticien.com/actualites/id/25434/l-afnic-conserve-la-gestion-des-fr.aspx**

Infos Réseau

- Le DDoS comme nouvelle forme de manifestation ?
  - http://www.security.nl/artikel/41978/1/D66_wil_DDoS-aanvallen_legaliseren.html
- CyberRoam pris en délit de DPI sur le réseau Tor
  - https://blog.torproject.org/blog/security-vulnerability-found-cyberoam-dpi-devices-cve-2012-3372
  - "CyberRoam vous sécurise"
    - http://blog.cyberoam.com/2012/07/ssl-bridging-cyberoam-approach/
- Les propriétaires de routeurs Cisco/Linksys migrés de force vers "Cisco Connect Cloud"
  - Modèles E2700, E2500 et E4500
    - http://www.extremetech.com/computing/132142-ciscos-cloud-vision-mandatory-monetized-and-killed-at-their-discretion
- Encore un bug BGP ?
  - https://isc.sans.edu/diary.html?storyid=13579
- L'Ethiopie interdit toute forme de VoIP
  - Y compris Skype

Infos Unix

- **(Principales) faille(s)**
  - **De nombreuses implémentation malloc() vulnérables**
    - **L'arrondi provoque un *integer overflow***
      - **http://permalink.gmane.org/gmane.comp.security.oss.general/7812**
  - **Sendmail sur AIX exécute le ".forward" en "root"**
    - **http://aix.software.ibm.com/aix/efixes/security/sendmail1_advisory.asc**
  - **Problème de gestion des clés GPG dans APT**
    - **https://lists.ubuntu.com/archives/ubuntu-security-announce/2012-June/001721.html**

Infos Unix

- ***One Leap Second to rule them all***
  - **http://serverfault.com/questions/403732/anyone-else-experiencing-high-rates-of-linux-server-crashes-during-a-leap-second**
  - **http://www.wired.com/wiredenterprise/2012/07/leap-second-bug-wreaks-havoc-with-java-linux/**

Infos Unix

- **Autre**
  - **Linus Torvalds remporte le "Millenium Prize"**
    - **http://www.lemonde.fr/technologies/article/2012/06/14/le-createur-de-linux-remporte-le-millennium-technology-prize_1718049_651865.html**

Failles

- **Publications ZDI (sans date)**
  - **Internet Explorer (pwn2own)**
    - **ZDI-12-093**
  - **Apple QuickTime**
    - **ZDI-12-095, ZDI-12-103, ZDI-12-105 , ZDI-12-107, ZDI-12-108, ZDI-12-109**
  - **Mozilla FireFox**
    - **ZDI-12-110**
  - **HP Data Protector**
    - **ZDI-12-096, ZDI-12-097, TPTI-12-06**
  - **SAP Netweaver ABAP**
    - **ZDI-12-104, ZDI-12-111, ZDI-12-112**

Failles

- Un nouveau programme d'achat de failles
  - … par des anciens de ZDI (Aaron Portnoy & al.)
    - https://www.exodusintel.com/eip/
- Principales applications
  - FireFox < 13.0.1, ThunderBird < 13.0.1
  - Java < 1.6.33, < 1.7.05
    - Les utilisateur de Java 6 sont automatiquement mis à jour en Java 7
    - Seul problème: cette version est incompatible avec le client Oracle
      - http://www.linformaticien.com/actualites/id/25252/oracle-il-faut-desactiver-la-mise-a-jour-automatique-de-java-7.aspx
  - Evasion de l'hyperviseur Xen
    - La faille était dans l'implémentation Intel vs. documentation AMD
      - http://blog.xen.org/index.php/2012/06/13/the-intel-sysret-privilege-escalation/
    - … et affecte de nombreux systèmes (*BSD, Windows 7, …)
  - Adobe ColdFusion
    - http://www.adobe.com/support/security/bulletins/apsb12-15.html

Failles

- Pidgin < 2.10.6
  - "Plain stack overflow"
    - http://www.pidgin.im/news/security/index.php?id=64
- VMWare
  - Un fichier de checkpoint corrompu peut conduire à l'exécution de code
    - http://www.vmware.com/security/advisories/VMSA-2012-0011.html
  - Intéressant à exploiter chez les fournisseurs de "Cloud" …

Failles 2.0

- La plupart des équipements médicaux ne sont pas à l'heure
  - http://www.economist.com/blogs/babbage/2012/05/medical-devices
- Paypal lance son "bug bounty"
  - https://cms.paypal.com/cgi-bin/marketingweb?cmd=_render-content&content_ID=security/reporting_security_issues

Sites piratés

- Simplement en panne
  - En panne
    - Amazon AWS (à cause des orages)
    - Salesforce
- Les sites piratés du mois
  - Wikileaks "Syria Files"
    - http://wikileaks.org/syria-files/
  - Anonymous #OpSaveTheArtic
    - Victimes: Exxon, Shell, BP, Gazprom, Rosneft
  - Anonymous #OpINDECT
    - "INtelligent information system supporting observation, searching and DEteCTion for security of citizens in urban environment"
      - http://reflets.info/oui-indect-a-bien-ete-p0wn3d/
  - Anonymous #OpJapan
    - http://thehackernews.com/2012/06/anonymous-hacks-japanese-government.html

Sites piratés

- L'armée indienne piratée par les chinois
  - http://thehackernews.com/2012/07/indian-navy-computers-hacked-by-chinese.html
- Environ 79 banques
  - http://news.cnet.com/8301-1009_3-57455693-83/hacker-claims-breach-of-79-banks-releases-customer-data/
- CACert.org laisse trainer ses mots de passe sur un post-it
  - https://lists.cacert.org/wws/arc/cacert-systemlog/2012-06/msg00012.html

- La question en pointe
  - Faut-il contre-attaquer ?
    - http://www.reuters.com/article/2012/06/17/us-media-tech-summit-cyber-strikeback-idUSBRE85G07S20120617

Malwares, spam et fraudes

- Facebook va alerter les victimes de DNSChanger
  - https://www.facebook.com/notes/facebook-security/notifying-dnschanger-victims/10150833689760766
- Rappel: les serveurs de DNSChanger ont été éteints le 9 juillet
- "Find and Call": un malware disponible sur Google Play et AppStore
  - http://www.securelist.com/en/blog/208193641/Find_and_Call_Leak_and_Spam
- Un virus en AutoLISP pour AutoCAD
  - … envoie tous les plans en Chine
    - http://blog.eset.com/2012/06/21/acadmedre-10000s-of-autocad-files-leaked-in-suspected-industrial-espionage
- Le FBI arrête le groupe de *carders* "UGNazi"
  - http://zataz.com/news/22255/
- Le KGB arrête le *bot herder* "Hermes"
  - Aussi connu sous le nom de "Arashi"
  - Quid du botnet ?
    - http://zataz.com/news/22257/Hermes--Arashi--bot.html

Malwares, spam et fraudes

- Faille exploitable à distance dans le serveur C&C de Poison Ivy
  - http://badishi.com/own-and-you-shall-be-owned/
- L'auteur de DarkComet jette l'éponge
  - http://www.darkcomet-rat.com/downloaddc.dc
- Un auteur de virus intègre un module de chat
  - … qui lui permet de communiquer avec les éditeurs antivirus
    - http://blogs.avg.com/news-threats/chatted-hacker-virus/
- Très bonne offre d'emploi
  - http://www.reddit.com/r/ReverseEngineering/comments/vxmzr/rreverseengineerings_q3_2012_hiring_thread/
- L'échec des antivirus
  - http://blog.ioactive.com/2012/06/inside-flame-you-say-shell32-i-say.html
  - http://www.zdnet.fr/actualites/flame-un-echec-collectif-pour-l-industrie-antivirus-39772859.htm

Actualité (francophone)

- L'ANSSI publie un guide sur la sécurité des SCADA
  - http://www.ssi.gouv.fr/fr/anssi/publications/communiques-de-presse/l-anssi-publie-un-guide-sur-la-cybersecurite-des-systemes-industriels.html
- L'ANSSI publie son outil d'audit AD
  - https://github.com/ANSSI-FR/AD-permissions
- L'antivirus français est sur les rails
  - Prévu pour 2014
    - http://www.davfi.fr/
- Le CLUSIF publie son rapport annuel sur les menaces
  - https://www.clusif.asso.fr/fr/production/ouvrages/pdf/CLUSIF-Rapport-2012.pdf
- ATOS n'est pas *fair play* avec ses outils de vote électronique
  - http://www.numerama.com/magazine/22972-atos-met-en-demeure-numerama-de-supprimer-son-document-sur-le-vote-electronique.html

Actualité (francophone)

- **Activité de la CNIL**
  - **Fiche pratique sur la notification de violation de données à caractère personnel**
    - **http://www.cnil.fr/en-savoir-plus/fiches-pratiques/fiche/accessible/non/article/la-notification-des-violations-de-donnees-a-caractere-personnel/**
  - **Guide pour gérer les risques sur la vie privée**
    - **http://www.cnil.fr/nc/la-cnil/actualite/article/article/deux-nouveaux-guides-securite-pour-gerer-les-risques-sur-la-vie-privee/**
  - **Conseils sur le Cloud**
    - **http://www.cnil.fr/nc/la-cnil/actualite/article/article/cloud-computing-les-conseils-de-la-cnil-pour-les-entreprises-qui-utilisent-ces-nouveaux-services/**
  - **Avertissement à YATEDO**
    - **http://www.cnil.fr/fileadmin/documents/approfondir/deliberations/Formation_contentieuse/Deliberation_2012-156_YATEDO_FRANCE.pdf**
  - **Avertissement à EURO INFORMATION (CIC)**
    - **http://www.cnil.fr/nc/la-cnil/actualite/article/article/defaut-de-securite-de-donnees-confidentielles-avertissement-pour-la-filiale-euro-information/**

Actualité (francophone)

- https://www.google.fr/search?q=site%3A*.gouv.fr+index+of
  - Accessoirement: l'ANSSI recrute ☺
- Le futur permis de conduire aura une puce
  - http://www.legifrance.gouv.fr/affichTexte.do;jsessionid=?cidTexte=JORFTEXT000026083508&dateTexte=&oldAction=rechJO&categorieLien=id
- "Arrêté du 3 juillet 2012 relatif à la protection du potentiel scientifique et technique de la nation"
  - http://www.legifrance.gouv.fr/affichTexte.do;jsessionid=?cidTexte=JORFTEXT000026140136&dateTexte=&oldAction=rechJO&categorieLien=id

Actualité (francophone)

- HADOPI a envoyé 1 million d'avertissements
  - Soit 4% des internautes
    - http://www.hadopi.fr/sites/default/files/page/pdf/Newsletter_juillet_2012.pdf

- La DCSSI vous informe
  - http://www.youtube.com/watch?v=LAuIfoWtXZk&feature=plcp
  - http://www.youtube.com/watch?v=hNuc1cQuubY&feature=plcp
  - http://www.youtube.com/watch?v=GK0HyRsL7zA&feature=plcp
  - …

Actualité (francophone)

- Du WiFi (sponsorisé) dans certaines stations de métro
- … et bientôt la 3G !
  - SFR a obtenu le marché
- SFR passe à l'EAP-SIM
- Orange déploie la 4G en test à Marseille
    - http://www.freenews.fr/spip.php?article12204
  - L'iPhone 5 ne sera probablement pas compatible …
    - http://www.pcinpact.com/news/71840-apple-iphone-5-incompatible-4g.htm
- Orange fournit des cartes SIM "NFC ready"
    - http://www.numerama.com/magazine/23035-orange-va-fournir-des-cartes-sim-nfc-a-ses-abonnes.html
- Le Minitel s'est éteint le 30 juin 2012
    - http://ripminitel.tumblr.com/
  - Sauf le 3618
  - 3615 ULLA faisait encore 21,000 visites/mois
    - http://www.rue89.com/rue89-eco/2012/06/29/gagnait-encore-de-largent-avec-le-minitel-233322

Actualité (francophone)

- Google rejoint le Syntec Numérique
  - http://www.linformaticien.com/actualites/id/25212/google-france-rejoint-le-syntec-numerique.aspx
- Alter Way remporte le marché de support des logiciels libres pour les ministères française
- Un "bug informatique" donne 50% de réduction sur tout le catalogue des 3 Suisses
  - http://www.linformaticien.com/actualites/id/25207/bug-des-3-suisses-que-dit-la-loi.aspx

Actualité (anglo-saxonne)

- "ICS CERT Incident Summary Report 2009-2011"
  - Nombre d'attaques en hausse: de 9 à 198 en 2 ans
    - http://www.us-cert.gov/control_systems/pdf/ICS-CERT_Incident_Response_Summary_Report_09_11.pdf
    - http://makaseh.wordpress.com/2012/06/30/u-s-critical-infrastructure-cyberattack-reports-jump-dramatically/

- Harris recrute des chercheurs de failles et des développeurs d'exploits
  - Source: VUPEN ☺
    - http://www.govcomm.harris.com/crucial-security/io-exploit-development.asp

- Les drones survolant les USA peuvent être piratés pour moins de $1,000
    - http://rt.com/usa/news/texas-1000-us-government-906/

Actualité (européenne)

- ACTA rejeté au parlement
- Revendre des licences logicielles est légal
  - http://www.linformaticien.com/actualites/id/25508/revendre-des-licences-logicielles-est-legal.aspx
- Opinion de la CNIL européenne sur un "Cybercrime Center" européen
  - http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-06-29_European_Cybercrime_Center_EN.pdf
- Le CERN confronté à l'absence de réglementation européenne claire sur la protection des données dans le Cloud
  - http://www.lemondeducloud.fr/lire-le-projet-cloud-du-cern-freine-par-le-retard-de-la-legislation-europeenne-49355.html

Actualité (Google)

- **Résumé de Google I/O**
  - Google 4.1 "Jelly Bean"
    - NFC
    - Les applications seront chiffrées et liées au terminal
  - Google fabriquera sa propre tablette (Nexus 7)
    - Distribuée lors de la conférence
    - … et déjà revendue sur eBay
  - Nexus Q
    - Une boite noire … équivalent de l'Apple TV actuelle
  - Google Docs bientôt disponible "offline"
  - Google Drive sur iOS
  - Google Glass
    - $1500 pour des lunettes de réalité augmentée
  - Google Brain
  - Chrome sur iOS
    - … mais le moteur est celui de Safari
  - Google+ sur iPad pour bientôt

Actualité (Google)

- Google Now
  - … vous veut du bien
    - http://www.lefigaro.fr/hightech/2012/06/27/01007-20120627ARTFIG00759-google-veut-deviner-ce-dont-vous-avez-besoin.php
    - http://www.infoworld.com/d/security/google-now-creates-concern-among-security-experts-196699
- Google Compute Engine
  - L'IaaS de Google
- Flash Player non supporté sur Android 4.1
  - Et retiré de Google Play à partir du 15 août 2012

Actualité (Google)

- Chrome disponible en version "Metro" (Windows 8)
- Quelques failles dans Chrome …
  - http://blog.chromium.org/2012/06/tale-of-two-pwnies-part-2.html
  - http://www.garage4hackers.com/f11/chrome-pdf-viewer-save-vulnerability-2396.html
- L'histoire d'un XSS dans les services Google
  - http://www.talesofacoldadmin.com/2012/06/18/the-page-at-accounts-google-com-says/
- Google lance une campagne mondiale pour le marriage homo (?!)
  - http://dot429.com/articles/2012/07/06/google-wants-the-world-to-legalize-love

Actualité (Apple)

- Un émulateur pour applications iOS sur BlackBerry PlayBook
  - http://www.appleinsider.com/articles/12/06/15/hacker_purportedly_demos_ios_apps_emulated_on_blackberry_playbook.html
- Il y a des virus sur Mac …
  - http://sophosnews.files.wordpress.com/2012/06/mac-osx-before-after.jpg
- … et il y a aussi des APT
  - https://www.securelist.com/en/blog/208193616/New_MacOS_X_backdoor_variant_used_in_APT_attacks
- Un nouvel AppStore en préparation
  - http://www.linformaticien.com/actualites/id/25210/le-nouvel-app-store-se-devoile.aspx
- Un nouvel iTunes en préparation
  - Il sera (peut-être) possible de partager la musique achetée avec ses amis

Actualité (crypto)

- "Padding Oracle" vs. Tokens
  - http://blog.cryptographyengineering.com/2012/06/bad-couple-of-years-for-cryptographic.html
  - http://hal.inria.fr/docs/00/70/47/90/PDF/RR-7944.pdf
- Non initialisé != aléatoire
  - Affecte: FreeBSD, Mac OS X …
    - http://kqueue.org/blog/2012/06/25/more-randomness-or-less/
- Analyse du chiffrement de disque Mac OS 10.7
  - http://eprint.iacr.org/2012/374
- Un système crypto à 923 bits attaqué en 178 jours
  - … avec seulement 252 cœurs
    - http://phys.org/news/2012-06-japanese-world-cryptanalysis-next-generation-cryptography.html
    - http://en.wikipedia.org/wiki/Pairing-based_cryptography
- Application d'entrainement à la crypto
  - https://github.com/SpiderLabs/CryptOMG

Actualité

- Conférences passées
  - Google I/O
    - https://developers.google.com/events/io/
  - HIP 2012
    - http://www.hackinparis.com/
- Conférences à venir
  - GreHack 2012
    - http://ensiwiki.ensimag.fr/index.php/GreHack_2012-Call_For_Presentation-english
  - RMLL 2012

Actualité

- Sorties logicielles
  - THC IPv6 1.9
    - http://www.thc.org/thc-ipv6/
  - IPv6 Toolbox
    - http://ipv6securitylab.org/ipv6toolbox.html
  - Volatility pour Mac OS X
  - John The Ripper 1.7.9-jumbo-6
    - Support GPU & MS-Office
  - OPA 1.0
    - http://blog.opalang.org/2012/06/announcing-opa-10.html
  - Secunia PSI 3.0
  - Lire sa carte NFC avec Android
    - https://code.google.com/p/readnfccc/
    - La copie: "paycardreader"
      - http://www.scmagazine.com.au/News/305881,android-app-steals-contactless-credit-card-data.aspx

Actualité

- Les leçons de DigiNotar
  - La sécurité déclarative ne fonctionne pas …
    - http://www.onderzoeksraad.nl/docs/persberichten/Press_release_DigiNotar_280612_EN_opgemaakt.pdf
- Les douaniers israéliens peuvent vous demander votre mot de passe de messagerie
    - http://www.schneier.com/blog/archives/2012/06/israel_demandin.html
- L'Irlande abandonne les machines à voter
    - http://www.numerama.com/magazine/23129-l-irlande-se-debarrasse-de-ses-machines-a-voter.html
- Le vote électronique démasqué
  - Access + VBA …
    - http://www.bbvforums.org/forums/messages/7659/82111.html

Actualité

- Le gouvernement Australien perd un DVD de mots de passe
  - … envoyé par la poste sans chiffrement
    - http://www.itnews.com.au/News/307958,auscert-loses-passwords-to-govt-service.aspx
- Facebook rachète Face.com
- Dell rachète Quest Software
- RIM licencie encore 5000 personnes

Divers

- Un système de commande en ligne
  - … qui donne un accès RDP à ses clients
    - http://thedailywtf.com/Articles/The-Online-Ordering-System.aspx
- Le Boson de Higgs présenté en Comic Sans MS
    - http://www.theverge.com/2012/7/4/3136652/cern-scientists-comic-sans-higgs-boson
- Le site www.edelweb.fr a été mis à jour ☺

Divers

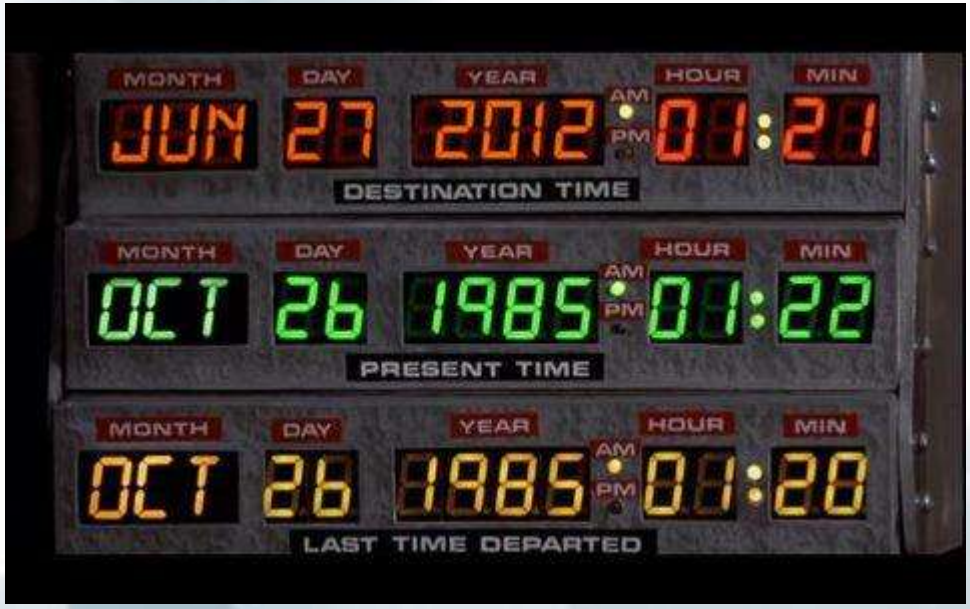
- L'échec de l'informatique

Divers

- L'échec du scam

Divers

- Back to the future

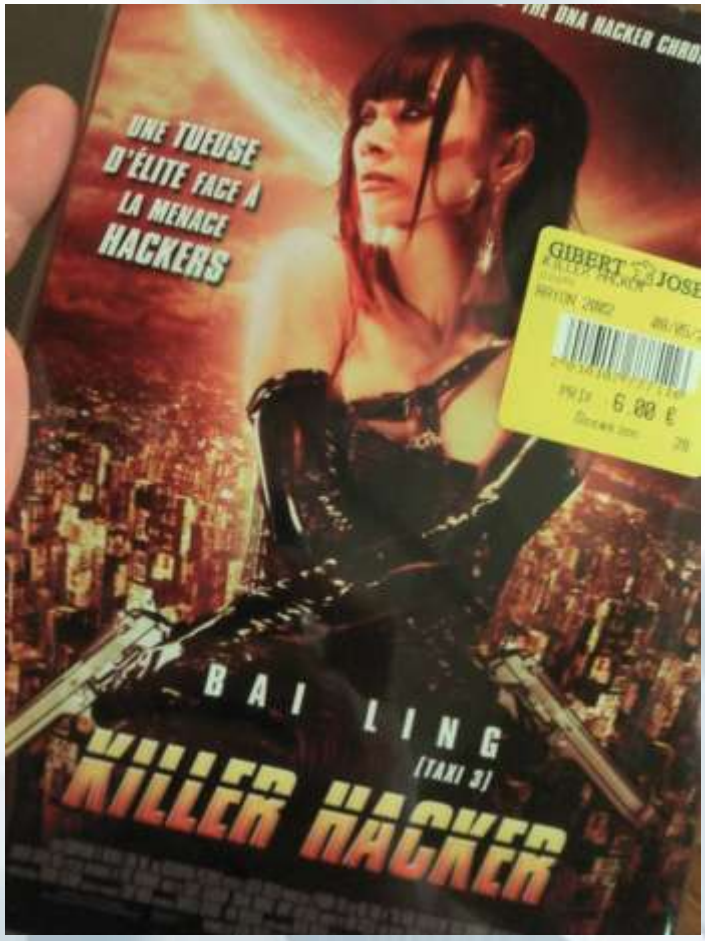


Divers

- **Un membre d'Anonymous arrêté**
  - **Grâce aux métadonnées de cette photo**

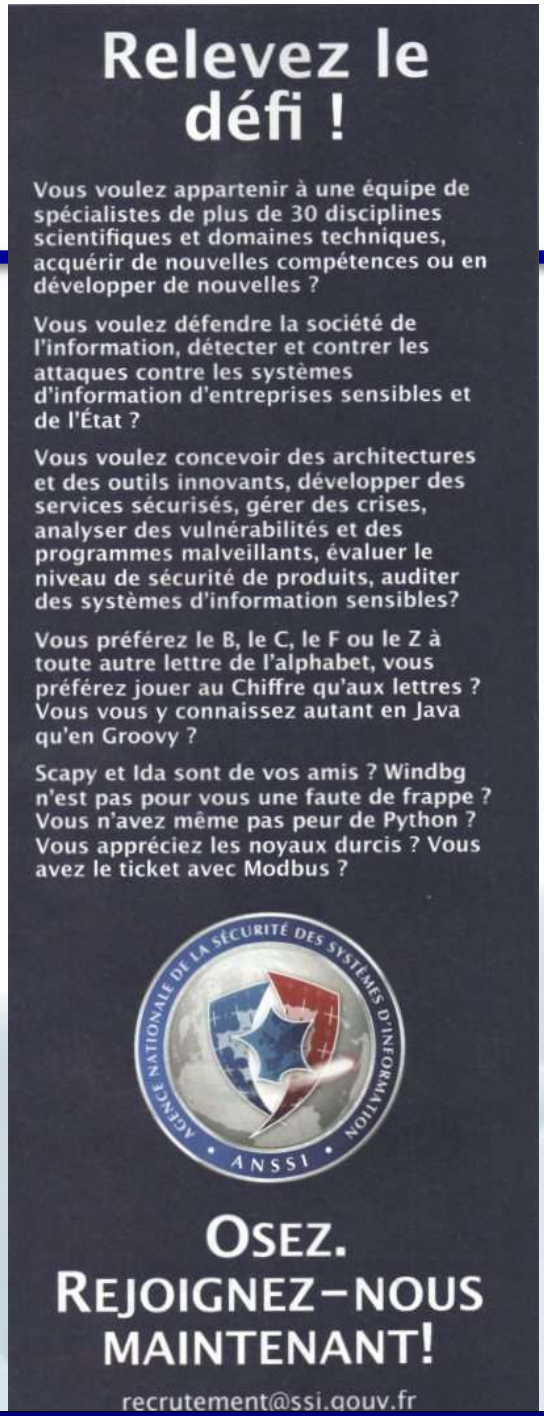
Divers

- La prochaine pub HSC (ou pas)
  - https://twitter.com/virtualabs/status/219159529991049216/photo/1



Divers

- Le saviez-vous ?
  - L'ANSSI recrute !
    - Source: MISC Magazine



Questions / réponses

- Questions / réponses
- Prochaine réunion
  - Mardi 11 septembre 2012