OSSIR
Groupe Paris

Réunion du 8 octobre 2013

Revue des dernières vulnérabilités

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

Avis Microsoft

- **Septembre 2013**

  - **MS13-067 Failles SharePoint (x10) [1]**
    - **Affecte: SharePoint et Office Web Apps (toutes versions supportées)**
    - **Exploit:**
      - **Déni de service**
        - **http://blog.csnc.ch/2013/09/microsoft-security-bulletin-ms13-067-critical/#!**
      - **XSS**
        - **http://www.vulnerability-lab.com/get_content.php?id=812**
      - **Elévation de privilèges**
      - **Exécution de code sous l'identité W3WP**
    - **Crédits:**
      - **Will Dormann / CERT/CC**
      - **Alexandre Herzog**
      - **Benjamin Kunz Mejri / Vulnerability Research Laboratory**
      - **Mateusz Jurczyk, Ivan Fratric & Ben Hawkes / Google Security Team (x5)**

  - **MS13-068 Faille Outlook (x1) [2]**
    - **Affecte: Outlook 2007 et 2010**
    - **Exploit: exécution de code à la prévisualisation d'un message**
      - **Lors du traitement des données S/MIME**
    - **Crédits: Alexander Klink / n.runs AG**

Avis Microsoft

- MS13-069 Failles IE (x10) [1]
  - Affecte: IE (toutes versions supportées, sauf IE 11)
  - Exploit: exécution de code à l'ouverture d'une page Web malformée
  - Crédits:
    - Jose Antonio Vazquez Gonzalez + ZDI (x3)
    - Arthur Gerkis + ZDI (x4)
    - Ivan Fratric & Ben Hawkes / Google Security Team
    - Peter 'corelanc0d3r' Van Eeckhoutte / Corelan + ZDI
    - Anonymous + ZDI

- MS13-070 Faille OLE (x1) [1]
  - Affecte: Windows XP et 2003
  - Exploit: exécution de code à l'ouverture d'un composant OLE malformé
  - Crédits: G. Geshev + ZDI

Avis Microsoft

- **MS13-071 Faille dans le support des thèmes (x1) [1]**
  - **Affecte: Windows XP, 2003, Vista, 2008**
  - **Exploit: exécution de code à l'ouverture d'un fichier ".theme" malformé**
  - **Crédits: Eduardo Prado + VeriSign iDefense Labs**

- **MS13-072 Failles Office (x13) [1]**
  - **Affecte: Office (toutes versions supportées, sauf 2013 et 2011 pour Mac)**
  - **Exploit:**
    - **Faille XXE**
    - **Corruptions mémoire multiples dans Word**
  - **Crédits:**
    - **Timur Yunusov, Alexey Osipov & Ilya Karpov / Positive Technologies**
    - **Mateusz Jurczyk, Ivan Fratric & Ben Hawkes / Google Security Team (x12)**

Avis Microsoft

- MS13-073 Failles Excel (x3) [3]
  - Affecte: Excel (toutes versions supportées, y compris Mac)
  - Exploit:
    - Faille XXE
    - Corruptions mémoire multiples dans Word
  - Crédits:
    - Will Dormann / CERT/CC (x2)
    - Timur Yunusov, Alexey Osipov & Ilya Karpov / Positive Technologies

- MS13-074 Failles Access (x3) [1]
  - Affecte: Access (toutes versions supportées, sauf 2003)
  - Exploit: corruptions mémoire multiples dans Access
  - Crédits: Kaveh Ghaemmaghami / Secunia SVCRP (x3)

Avis Microsoft

- **MS13-075 Faille dans l'IME Chinois sous Office (x1) [1]**
  - **Affecte: Office 2010 SP1**
  - **Exploit: élévation de privilèges**
  - **Crédits: Wei Wang / VulnHunt**

- **MS13-076 Failles noyau (x7) [1]**
  - **Affecte: Windows (toutes versions supportées, sauf 8.1 et 2012 R2)**
  - **Exploit: élévation de privilèges locale**
  - **Crédits:**
    - **Gynvael Coldwind & Mateusz "j00ru" Jurczyk / Google Inc (x5)**
    - **Mateusz "j00ru" Jurczyk / Google Inc**
    - **Guo Pengfei / Qihoo 360 Security Center**

Avis Microsoft

- **MS13-077 Faille dans SCM (x1) [2]**
  - **Affecte: Windows 7 et 2008 R2**
  - **Exploit: "double free" dans le Service Control Manager (SCM)**
  - **Crédits: n/d**

- **MS13-078 Faille FrontPage (x1) [3]**
  - **Affecte: FrontPage 2003 SP3**
  - **Exploit: lecture de fichiers arbitraires lors d'un traitement XML**
  - **Crédits: Timur Yunusov / Positive Technologies**

- **MS13-079 Faille Active Directory (x1) [3]**
  - **Affecte: AD et AD LDS (toutes versions supportées, sauf XP, 2003 et 2012 R2)**
  - **Exploit: déni de service distant via une requête LDAP (anonyme)**
  - **Crédits: n/d**

Avis Microsoft

- **Advisories**
  - **Q2755801 Flash Player (intégré à IE10+)**
    - **V15.0: nouvelle version**
  - **Q2887505 Faille IE (exploitée dans la nature contre IE8 et IE9)**
    - **V1.0: publication de l'avis**

Avis Microsoft

- **Prévisions pour Octobre 2013**
  - **8 bulletins**
    - **7 critiques: Windows, .NET, IE**
    - **Dont un 0day en cours d'exploitation**
      - **Opération "Deputy Dog"**
      - **Disponible depuis une semaine dans Metasploit**
    - **1 important: Office, SilverLight**

- **Failles à venir**
  - **N/A**

- **Retour sur des failles antérieures**
  - **N/A**

Avis Microsoft

- **Révisions**
  - **MS13-023**
    - **V1.2: changement documentaire**
  - **MS13-055**
    - **V1.3: ajout d'un CVE**
  - **MS13-063**
    - **V1.2: changement documentaire**
  - **MS13-067**
    - **V1.1: le *workaround* ne fonctionne pas**
    - **V1.2: changement dans la logique de détection**
  - **MS13-068**
    - **V1.1: ajout d'un *workaround***
  - **MS13-072**
    - **V1.1: changement dans la logique de détection ; ajout d'un problème connu**
  - **MS13-073**
    - **V1.1: changement dans la logique de détection ; ajout d'un problème connu**
  - **MS13-074**
    - **V1.1: changement dans la logique de détection**
  - **MS13-077**
    - **V1.1: ajout d'un problème connu**

Infos Microsoft

- **Sorties logicielles**
  - **Message Analyzer**
    - **La suite de Network Monitor**
      - **http://blogs.technet.com/b/messageanalyzer/archive/2013/09/25/message-analyzer-has-released-a-new-beginning.aspx**

Infos Microsoft

- **Autre**
  - **Sorties de Surface 2 et Surface Pro 2 le 22 octobre prochain**

Infos Réseau

- **(Principales) faille(s)**
  - **Cisco CUCM IM**
    - **cisco-sa-20130821-cup**
      - **DoS**
  - **Cisco Webex**
    - **cisco-sa-20130904-webex**
      - **Faille dans le support des formats WRF et ARF par le lecteur**
  - **Cisco Prime Central**
    - **cisco-sa-20130821-hcm**
      - **DoS multiples**
    - **cisco-sa-20130918-pc**
      - **Contournement de l'authentification …**
  - **Cisco Prime Data Center**
    - **cisco-sa-20130918-dcnm**
      - **"Cisco Prime DCNM Information Disclosure Vulnerability"**
      - **"Cisco Prime DCNM Remote Command Execution Vulnerabilities"**
      - **"Cisco Prime DCNM XML External Entity Injection Vulnerability"**

Infos Réseau

- Cisco IOS
  - cisco-sa-20130925-ipv6vfr
    - DoS causé par la "fragmentation virtuelle" sur IPv6 …
  - cisco-sa-20130925-nat
    - DoS dans le support de la NAT
  - cisco-sa-20130925-cce
    - DoS dans le support HTTP par le "Zone Based Firewall"
  - cisco-sa-20130925-ntp
    - DoS dans le support multicast NTP
  - cisco-sa-20130925-wedge
    - DoS dans le support T1/E1
  - cisco-sa-20130925-dhcp
    - DoS dans le support DHCP …
  - cisco-sa-20130925-ike
    - DoS dans le support IKE par fuite mémoire
  - cisco-sa-20130925-rsvp
    - DoS dans le support RSVP

- Cisco IOS XR
  - cisco-sa-20131002-iosxr
    - DoS

Infos Réseau

- **Autres infos**
  - **N/A**

Infos Unix

- **(Principales) faille(s)**
  - **Ruby On Rails**
    - **eval(cookie) … *what could possibly go wrong?***
      - **http://www.sitepoint.com/rails-security-pitfalls/**
  - **Struts < 2.3.15.2**
    - **2 failles de sécurité corrigées**
      - **http://struts.apache.org/release/2.3.x/docs/version-notes-23152.html**
  - **Injection SQL dans Zabbix**
    - **Requière une authentification … sauf si le mode "guest" est activé**
      - **https://www.sec-consult.com/en/Vulnerability-Lab/Advisories.htm#a135**
      - **https://support.zabbix.com/browse/ZBX-7091**

Infos Unix

- **Autres infos**
  - **N/A**

Failles

- **Principales applications**

  - **ShockWave (x2)**
    - **http://www.adobe.com/support/security/bulletins/apsb13-23.html**
  - **Flash Player (x4) et Adobe AIR**
    - **http://www.adobe.com/support/security/bulletins/apsb13-21.html**
  - **Adobe Reader (x8)**
    - **http://www.adobe.com/support/security/bulletins/apsb13-22.html**

  - **Java < 1.7.40**
    - **Version précédente: 1.7.25**
      - **http://www.oracle.com/technetwork/java/javase/7u40-relnotes-2004172.html**
  - **WireShark < 1.10.2**

Failles

- **WatchGuard**
  - **http://funoverip.net/2013/09/cracking-watchguard-passwords/**
  - **http://watchguardsecuritycenter.com/2013/09/24/watchguard-password-cracking-should-i-be-worried/**

- **Citrix NetScaler (DoS)**
  - **https://www.sec-consult.com/en/Vulnerability-Lab/Advisories.htm#a134**

Failles 2.0

- Piratage d'une agence Barclays
  - Avec un KVM et un modem 3G
    - http://www.lefigaro.fr/flash-eco/2013/09/20/97002-20130920FILWWW00300-gb-8-hommes-piratent-barclays.php

- Le bug bounty Yahoo ?
  - Un T-Shirt à 12$50
    - http://grahamcluley.com/2013/09/serious-yahoo-bug/
    - http://yahoodevelopers.tumblr.com/post/62953984019/so-im-the-guy-who-sent-the-t-shirt-out-as-a-thank-you

Sites piratés

- **Les sites piratés du mois (liste partielle)**
  - **Adobe**
    - **Intrusion au travers de ColdFusion**
    - **3M CC … et du code source (ex. Adobe Reader XI)**
      - **http://krebsonsecurity.com/2013/10/adobe-to-announce-source-code-customer-data-breach/**
  - **Belgacom**
    - **Piraté par … NSA + GCHQ**
      - **http://news.slashdot.org/story/13/09/20/1350224/snowden-docs-brits-hacked-accounts-of-belgian-it-admins**
      - **http://www.01net.com/editorial/603178/la-nsa-aurait-pirate-le-reseau-de-belgacom-pour-espionner-le-trafic-voix-et-data/**
      - **http://www.lemonde.fr/technologies/article/2013/09/21/les-britanniques-seraient-responsables-du-piratage-de-belgacom_3482143_651865.html**
  - **LeaseWeb**
    - **http://thehackernews.com/2013/10/worlds-largest-web-hosting-company_5.html**
  - **Vodafone Allemagne (2M comptes)**
  - **Le site de recrutement FireEye …**
    - **http://www.fireeye.com/blog/technical/cyber-exploits/2013/09/darkleech-says-hello.html**

Malwares, spam et fraudes

- DAVFI
  - Sortie de DavDroid (ou pas)
    - http://www.davfi.fr/davdroid.html
  - Présentation au Sénat le 17/10
    - https://twitter.com/zataz/status/378259319017324545

- La plateforme d'échange de bitcoins "Silk Road" démantelée par le FBI
  - Grâce aux failles dans TOR …
    - https://medium.com/p/d48995e8eb5a

- Le FBI loue des serveurs en France pour infiltrer le réseau TOR
    - http://www.numerama.com/magazine/27001-le-fbi-a-hacke-des-serveurs-situes-en-france-pour-diffuser-un-spyware.html

Malwares, spam et fraudes

- **FireEye publie "World War C"**
  - http://www.fireeye.com/resources/pdfs/fireeye-wwc-report.pdf
- **Symantec publie "Hidden Lynx"**
  - http://arstechnica.com/security/2013/09/meet-hidden-lynx-the-most-elite-hacker-crew-youve-never-heard-of/
  - http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/hidden_lynx.pdf
- **Kaspersky publie "Icefog"**
  - http://arstechnica.com/security/2013/09/for-hire-elite-cyber-mercenaries-adept-at-infecting-windows-and-macs/
  - http://www.securelist.com/en/analysis/204792307/The_Icefog_APT_Frequently_Asked_Questions
  - http://www.securelist.com/en/blog/208214064/The_Icefog_APT_A_Tale_of_Cloak_and_Three_Daggers
- **Des terminaux de paiement piratés**
  - Simply Market à Saclay
    - http://www.leparisien.fr/espace-premium/essonne-91/le-supermarche-victime-d-un-piratage-informatique-12-07-2013-2975615.php
- **McAfee recrute … sur Twitter**
  - https://twitter.com/ingridmara/status/380059399659610112

Actualité (francophone)

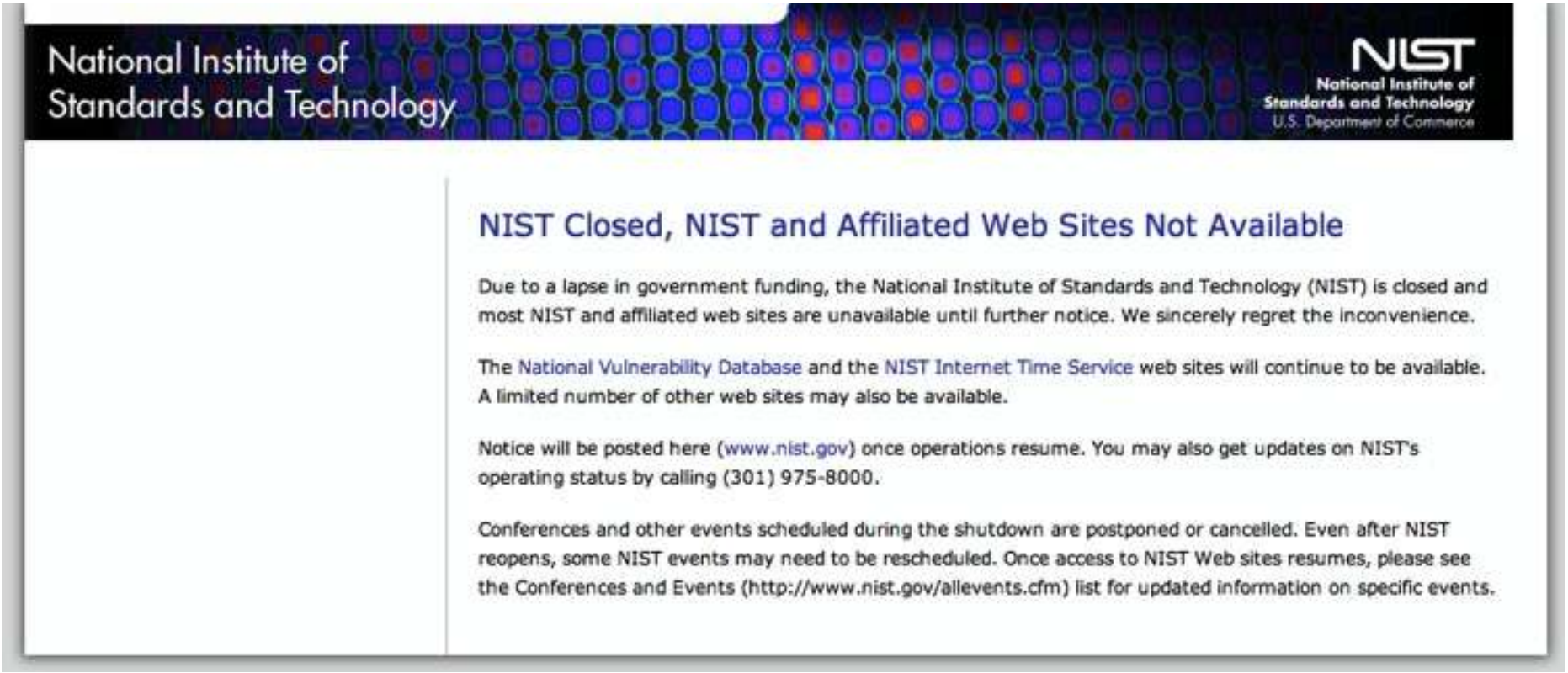
- **Un groupe de PME françaises lancent HexaTrust**
  - **http://www.hexatrust.com**
- **Bull lance le smartphone Hoox**
  - **Compter 2000€**
- **Les ministres français ne devraient pas utiliser de *smartphone* étranger**
  - **http://lexpansion.lexpress.fr/high-tech/cybersecurite-les-ministres-interdits-de-smartphones_400697.html**
- **Orange mesure les flux touristiques depuis ses BTS**
  - **http://www.lesechos.fr/journal20131004/lec2_pme_et_regions/0202888001805-orange-mesure-les-flux-touristiques-avec-precision-via-le-mobile-613562.php**
- **Numergy propose 2 mois d'essai gratuit**
  - **… mais il faut fournir une carte bleue**
  - **Note: le firewall est une option payante ☺**
    - **https://www.numergy.com/tarifs-cloud-simulateur-prix**

Actualité (francophone)

- **Nouvelle règle: un compte Paypal est un compte à l'étranger**
  - **http://www.linformaticien.com/actualites/id/30563/un-compte-paypal-doit-etre-declare-comme-un-compte-detenu-a-l-etranger.aspx**
- **Heureusement il existe maintenant un concurrent français: Paylib ☺**
  - **http://www.challenges.fr/economie/20130917.CHA4399/trois-banques-francaises-creent-un-concurrent-de-paypal.html**

Actualité (anglo-saxonne)

- "Shutdown" de l'administration américaine
  - Fermeture des services non critiques
  - … comme le NIST



Actualité (anglo-saxonne)

- **PRISM: une actualité sans fin …**
  - **Comment a fait Snowden ?**
    - http://www.computerweekly.com/news/2240205710/NSA-reveals-how-Snowden-accessed-secret-Prism-files
  - **Quand la NSA se moque d'Apple …**
    - **… et sa publicité 1984**
      - http://www.spiegel.de/fotostrecke/photo-gallery-spying-on-smartphones-fotostrecke-101201.html
  - **L'Europe suspend le partage des données SWIFT**
    - http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2013/2831%28RSP%29&l=en
    - **Pas sûr que ça change grand chose ☺**
      - http://www.01net.com/editorial/603118/la-nsa-espionne-aussi-les-reseaux-visa-et-mastercard/
  - **La NSA a des fournisseurs français**
    - **Ex. VUPEN et Systran**
      - http://www.lepoint.fr/editos-du-point/jean-guisnel/systran-ces-francais-qui-traduisent-le-monde-pour-la-nsa-18-09-2013-1732803_53.php
  - **John McAfee lance un produit d'anonymisation totale**
    - http://www.futuretensecentral.com

Actualité (anglo-saxonne)

- NSA vs. Google
  - https://s3.amazonaws.com/s3.documentcloud.org/documents/785152/166819124-mitm-google.pdf
- NSA vs. Linux
  - http://linux.slashdot.org/story/13/09/19/0227238/linus-torvalds-admits-hes-been-asked-to-insert-backdoor-into-linux
  - http://www.lemonde.fr/technologies/article/2013/09/19/le-gouvernement-americain-a-t-il-tente-de-mettre-un-acces-secret-dans-linux_3481314_651865.html
- NSA vs. TOR
  - http://www.theguardian.com/world/interactive/2013/oct/04/tor-high-secure-internet-anonymity
  - http://www.theguardian.com/world/interactive/2013/oct/04/egotistical-giraffe-nsa-tor-document
  - http://www.theguardian.com/world/2013/oct/04/tor-attacks-nsa-users-online-anonymity
  - http://fr.scribd.com/doc/166816957/corporate-partner
  - http://fr.scribd.com/doc/166819131/map
  - Utilisation des cookies pour le tracking
    - http://www.theguardian.com/world/interactive/2013/oct/04/tor-stinks-nsa-presentation-document
  - Carte des nœuds Tor
    - https://tormap.void.gr

Actualité (européenne)

- N/A

Actualité (Google)

- QuickOffice devient gratuit
  - Intégré avec Google Drive depuis le rachat par Google
  - Disponible sur Android et iOS

- Google Calico
  - Un projet pour devenir … immortel (encore en beta)
    - https://plus.google.com/+LarryPage/posts/Lh8SKC6sED1

Actualité (Apple)

- **iOS 7**
  - **Offre gratuitement iWorks, iMovie et iPhoto**
    - **Si vous activez votre *device* après le 1er septembre …**
  - **N'est plus vulnérable aux chargeurs (et autres accessoires) malveillants**
  - **Intègre MultiPath TCP**

- **… et s'avère vulnérable à un contournement du *lock screen* …**
  - **Corrigé par iOS 7.0.2**
    - **http://support.apple.com/kb/HT5957**

- **Touch ID "cassé" par le CCC**
    - **http://www.ccc.de/en/updates/2013/ccc-breaks-apple-touchid**

- **Failles**
  - **iTunes < 11.1**
    - **http://support.apple.com/kb/HT5936**
  - **Safari < 5.1.10**
    - **http://support.apple.com/kb/HT5921**
  - **Mac OS X < 10.8.5**
    - **http://support.apple.com/kb/HT5880**
    - **http://support.apple.com/kb/HT5964**
  - **Mac OS X Server < 2.2.2**
    - **http://support.apple.com/kb/HT5892**

Actualité (crypto)

- RSA: "n'utilisez plus le générateur d'aléa de la suite BSAFE"
  - Il est basé sur une courbe elliptique backdoorée par la NSA …
    - http://www.wired.com/threatlevel/2013/09/rsa-advisory-nsa-algorithm/
- Backdoorer le générateur d'aléa embarqué dans un Intel Ivy Bridge
    - http://arstechnica.com/security/2013/09/researchers-can-slip-an-undetectable-trojan-into-intels-ivy-bridge-cpus/
- Brevet Apple sur une backdoor cryptographique
    - http://cryptome.org/2013/09/apple-backdoor.pdf
- Le NIST est-il à la solde de la NSA ?
    - https://www.cdt.org/blogs/joseph-lorenzo-hall/2409-nist-sha-3
- En tous cas le doute s'installe …
    - http://www.mail-archive.com/cryptography@metzdowd.com/msg12325.html

Actualité (crypto)

- Sale temps pour les autorités de certification
  - NetCraft
    - http://news.netcraft.com/archives/2013/09/23/certificate-authorities-struggle-to-comply-with-baseline-requirements.html
  - Google
    - https://cabforum.org/pipermail/public/2013-September/002233.html

- Silent Circle
  - … n'utilise plus d'algorithmes américains
    - http://silentcircle.wordpress.com/2013/09/30/nncs/

- L'histoire de Lavabit
    - http://www.pcinpact.com/news/82727-lavabit-compte-dedward-snowden-a-destruction-serveurs.htm

Actualité

- **Conférences passées**
  - **Les Assises de la Sécurité 2013**
    - **#AssisesSI**
    - **http://bluenod.com/map/assisessi**
    - **http://si-vis.blogspot.fr/2013/10/assises-de-la-securite-monaco-vers.html**
    - **http://magazine.qualys.fr/marche-business/assises-2013-balkanisation/#!**
    - **http://www.globalsecuritymag.fr/Les-Assises-de-la-Securite-2013,20131009,40206.html**

- **Conférences à venir**
  - **ASFWS 2013**
  - **Hack.Lu 2013**
  - **GreHack 2013**
  - **BotConf 2013**
  - **…**

Actualité

- **Sorties logicielles**
  - **Nouvel outil d'audit Active Directory**
    - **https://bitbucket.org/iwseclabs/bta**
  - **Splunk 6.0**
  - **Kvasir**
    - **Un "meta" outil de pentest par Cisco**
      - **http://blogs.cisco.com/security/introducing-kvasir/**
  - **Projet Sonar**
    - **Rapid7 scanne Internet**
      - **https://community.rapid7.com/community/infosec/sonar/blog/2013/09/26/welcome-to-project-sonar**
  - **"LG Gate": le smartphone sécurisé selon LG**
    - **http://www.lgnewsroom.com/newsroom/contents/63953**

Actualité

- La cyberguerre fait des vrais morts
  - Le chef du cyberwarfare iranien assassiné
    - http://www.telegraph.co.uk/news/worldnews/middleeast/iran/10350285/Iranian-cyber-warfare-commander-shot-dead-in-suspected-assassination.html

- BlackBerry racheté par le fond d'investissement Fairfax Financial

Divers

- Un portage de NetBSD … en Haskell
  - http://metasepi.org
- Un kernel … en Rust
  - https://github.com/charliesome/rustboot
- Un browser … prouvé en Coq
  - http://goto.ucsd.edu/quark/
- J'ai ri
  - http://stackoverflow.com/questions/184618/what-is-the-best-comment-in-source-code-you-have-ever-encountered

Divers

- ***What could possibly go wrong ?***
  - **Source: https://www.trustico.fr/ssltools/match/cert-and-key-pem/verifier-compatibilite-certificat-et-cle-privee.php**

Questions / réponses

- Questions / réponses
- Prochaine réunion
  - Mardi 12 novembre 2013
- Prochain AfterWork
  - Mardi 22 octobre 2013
    - "Projet Ivy" (Fred Raynal / Quarkslab)
- Prochaine JSSI
  - Lundi 17 mars 2014
  - Profitez du combiné avec les GS-Days le mardi 18 mars
- N'hésitez pas à proposer des sujets et/ou des salles