OSSIR
Groupe Paris

Réunion du 10 décembre 2013

Revue des dernières vulnérabilités

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

Avis Microsoft

Novembre 2013

- MS13-088 Correctif cumulatif pour IE (x10) [1,2,3]
  - Affecte: IE 6 – 11
    - Sauf IE 11 pour Windows 7 / 2008 R2
  - Exploit:
    - Fuite d'information (contournement de la SOP)
    - Corruption mémoire conduisant à l'exécution de code
  - Crédits:
    - Simon Zuckerbraun + ZDI
    - Masato Kinugawa
    - Sergey Markov
    - Peter 'corelanc0d3r' Van Eeckhoutte / Corelan + ZDI
    - Stephen Fewer / Harmony Security + ZDI
    - lokihardt@ASRT + ZDI
    - Anonymous + VeriSign iDefense Labs
    - Anonymous + ZDI
    - Bo Qu / Palo Alto Networks (x3)

Avis Microsoft

- **MS13-089 Faille GDI+ (x1) [1]**
  - **Affecte: Windows (toutes versions supportées)**
  - **Exploit: "integer overflow" lors du traitement d'un fichier ".WRI" par WordPad**
  - **Crédits: Hossein Lotfi / Secunia Research**

- **MS13-090 Faille dans l'ActiveX "InformationCardSigninHelp" / "icardie.dll" (x1) [1]**
  - **Affecte: Windows (toutes versions supportées)**
  - **Exploit: exécution de code depuis une page HTML**
  - **Crédits:**
    - **ucq & Daiki Fukumori / Cyber Defense Institute, Inc.**
    - **iSIGHT Partners**
    - **Dan Caselden & Xiaobo Chen / FireEye**

Avis Microsoft

- MS13-091 Failles Office (x3) [1,3]
  - Affecte: Office (toutes versions supportées)
    - Sauf Compatibility Pack et Office 2011 pour Mac
  - Exploit: exécution de code à l'ouverture d'un fichier ".WPD" malformé
    - "Stack overflow", "heap overflow", …
  - Crédits:
    - Merliton
    - Will Dormann / CERT/CC (x2)

- MS13-092 Faille Hyper-V (x1) [1]
  - Affecte: Windows 8 / 2012
  - Exploit:
    - Exécution de code depuis une VM dans une autre VM
    - Déni de service de l'hôte
  - Crédits: Christian Weyer

Avis Microsoft

- **MS13-093 Fuite d'information dans AFD.SYS (x1) [3]**
  - **Affecte: Windows (toutes versions x64 supportées, sauf 8.1 / 2012 R2)**
  - **Exploit: fuite d'information sur la structure mémoire**
  - **Crédits: n/d**

- **MS13-094 Fuite d'information dans Outlook (x1) [3]**
  - **Affecte: Office 2007 / 2010 / 2013**
  - **Exploit: scan de ports à partir du champ AIA d'une signature S/MIME**
    - **http://blog.nruns.com/blog/2013/11/12/A-portscan-by-email-Alex/**
  - **Crédits: Alexander Klink / n.runs professionals GmbH**

- **MS13-095 Faille dans le support X.509 (x1) [3]**
  - **Affecte: Windows (toutes versions supportées)**
  - **Exploit: déni de service lors du traitement d'un certificat X.509 malformé**
  - **Crédits: James Forshaw / Context Information Security**

Avis Microsoft

- Advisories
  - Q2755801
    - V16.0: nouvelle mise à jour de Flash Player
  - Q2854544
    - V1.3: mise à jour des règles concernant les "Root CA"
  - Q2862152 Attaque "MITM" possible contre DirectAccess
    - V1.0: publication initiale
      - Crédit: Daniel Letkiewicz / Google
  - Q2868725 Ajout d'une clé de BdR permettant de désactiver l'algorithme RC4 (!)
    - V1.0: publication initiale

Avis Microsoft

- Q2880823 Déprécation de l'algorithme SHA-1 pour les "Root CA"
  - V1.0: publication initiale
- Q2896666 "0day" en cours d'exploitation dans un composant de traitement d'image
  - V1.1: détails sur les attaques en cours, et nouvelles solutions de contournement
- Q2914486 Elévation de privilèges locale sur Windows
  - V1.0: le composant NDPROXY sur Windows XP/2003 est vulnérable
    - http://www.fireeye.com/blog/technical/cyber-exploits/2013/12/cve-2013-33465065-technical-analysis.html
    - http://www.exploit-db.com/exploits/30014/
- Q2916652 Certificat IGC/A frauduleux
  - V1.0: publication initiale

Avis Microsoft

- **Prévisions pour Décembre 2013**
  - **11 bulletins (5 critiques, 6 importants)**
- **Failles à venir**
  - **DoS local sur Windows**
    - **http://pastebin.com/we0ZSQC0**
- **Retour sur des failles antérieures**
  - **MS13-052 (évasion .NET)**
    - **http://www.contextis.com/research/blog/Expressing_Yourself_Analysis_Dot_Net_Elevation_Pri/**

Avis Microsoft

- Révisions
  - MS13-067
    - V1.3: correction documentaire (nom de produit)
  - MS13-084
    - V1.1: correction documentaire (nom de produit)
  - MS13-085
    - V1.1: correction documentaire (mises à jour remplacées)

Infos Microsoft

- **Sorties logicielles**
  - **EMET 4.1**
  - **MBSA 2.3**
  - **IE 11 pour Windows Seven**
  - **Visual Studio 2013**
  - **Windows Azure Backup**
  - **HDInsight (Hadoop)**

Infos Microsoft

- **Autre**
  - **Security Intelligence Report (SIR) v15**
  - **Microsoft ouvre un centre de lutte contre le cybercrime**
    - **http://thenextweb.com/microsoft/2013/11/14/microsoft-opens-stunning-cybercrime-center-redmond-tackle-botnets-malware-ip-theft/**
  - **Microsoft Curah!**
    - **Un nouveau site de support communautaire**
      - **http://curah.microsoft.com/**
  - **Office 365 va bientôt pour chiffrer des emails (!)**
    - **Avec l'algorithme Exchange Hosted Encryption**
      - **http://thenextweb.com/microsoft/2013/11/22/starting-early-2014-you-can-send-encrypted-emails-in-microsoft-office-365-to-anyone/**
  - **La Chine demande une extension du support Windows XP**
    - **http://www.techweb.com.cn/it/2013-12-03/1365350.shtml**

Infos Microsoft

- **Best. Goodie. Ever.**
  - **http://www.microsoftstore.com/store/msusa/en_US/pdp/Scroogled-Keep-Calm-Mug/productID.291428700**

Infos Réseau

- **(Principales) faille(s)**
  - **Faille Cisco TelePresence VX Clinical Assistant (?!)**
    - **cisco-sa-20131106-tvxca**
  - **Faille SIP dans Cisco IOS**
    - **cisco-sa-20131106-sip**
  - **Faille dans Cisco WAAS**
    - **cisco-sa-20131106-waasm**

Infos Réseau

- **Autres infos**
  - **Détournement de trafic via BGP**
    - **Ceci n'est pas un exercice**
      - **http://www.bortzmeyer.org/bgp-shunt.html**

Infos Unix

- **(Principales) faille(s)**
  - **put_user/get_user sont non fiables sur Linux/ARM**
    - **Résultat: exploit 'vroot' sur Android**
      - **https://www.codeaurora.org/projects/security-advisories/missing-access-checks-putusergetuser-kernel-api-cve-2013-6282**
  - **PHP < 5.5.6**
    - **http://www.php.net/ChangeLog-5.php#5.5.6**
  - **GitLab**
    - **http://blog.gitlab.org/multiple-critical-vulnerabilities-in-gitlab/**
  - **Ruby**
    - **"Heap overflow" lors de la conversion d'une chaine en flottant**
    - **Pas de patch pour Ruby 1.8**
      - **https://www.ruby-lang.org/en/news/2013/11/22/heap-overflow-in-floating-point-parsing-cve-2013-4164/**

Infos Unix

- Autres infos
  - La NSA tente de backdoorer Linux
    - http://www.pcinpact.com/news/84466-oui-nsa-a-bien-essaye-dintegrer-porte-derobee-dans-linux.htm
  - L'Open Source n'est pas plus sécurisé ni plus réactif …
    - https://community.rapid7.com/community/metasploit/blog/2013/10/29/seven-foss-disclosures-part-one

Failles

Principales applications

- Adobe Flash Player / Adobe AIR (x2)
  - Faille exploitée dans la nature
    - https://www.adobe.com/support/security/bulletins/apsb13-26.html
- Adobe ColdFusion 9 et 10
  - XSS
  - Contournement de l'authentification (ColdFusion 10 uniquement)
    - http://www.adobe.com/support/security/bulletins/apsb13-27.html
- Firefox < 25.0.1
    - http://xorl.wordpress.com/2009/10/31/cve-2009-1563-mozilla-firefox-floating-point-heap-overflow/
- Chrome < 31
  - Support AES-GCM
  - 25 failles corrigées
    - http://googlechromereleases.blogspot.com/2013/11/stable-channel-update.html

Failles

- Nvidia
  - Elévation de privilèges locale dans tous les drivers (sauf Tegra)
    - http://nvidia.custhelp.com/app/answers/detail/a_id/3377
- VMWare
  - Elévation de privilèges au sein de l'hôte Linux
    - http://www.vmware.com/security/advisories/VMSA-2013-0013.html
- Client BlackBerry 10
  - "DNS Rebinding" sur le serveur NGINX local
    - http://blog.cmpxchg8b.com/2013/11/qnx.html

Failles 2.0

- La caméra de votre smartphone
  - … peut servir à enregistrer votre PIN
    - http://www.bbc.co.uk/news/technology-24897581

- Quand la télé vous regarde …
    - http://www.tomshardware.fr/articles/lg-televiseur,1-46261.html

Sites piratés

- **Les sites piratés du mois (liste partielle)**
  - **Cupid Media (Janvier 2013)**
    - **On sait maintenant qu'il y avait 42M de mots de passe en clair …**
      - **http://krebsonsecurity.com/2013/11/cupid-media-hack-exposed-42m-passwords/**
  - **MacRumors (860,000 comptes)**
    - **http://www.macrumors.com/2013/11/12/macrumors-forums-security-leak/**
  - **J P Morgan Chase (465,000 utilisateurs)**
    - **http://nakedsecurity.sophos.com/2013/12/05/jp-morgan-chase-owns-up-to-data-breach-465000-customers-at-risk/**
  - **Bitcash.cz**
    - **http://thehackernews.com/2013/11/bitcashcz-bitcoin-exchange-hacked-money.html**

Sites piratés

- 2M de comptes divers volés par le botnet Pony
  - http://blog.spiderlabs.com/2013/12/look-what-i-found-moar-pony.html
- The Pirate Bay change de main
  - https://twitter.com/Anon_Central/status/402407735418814464/photo/1
- Guess What
  - En fait, Anonymous n'est pas mort
    - http://www.theverge.com/2013/11/15/5109462/anonymous-has-reportedly-been-hacking-us-government-computers-for-almost-a-year
- GitHub
  - Brute-force des comptes utilisateur depuis 40,000 adresses IP source
    - https://github.com/blog/1698-weak-passwords-brute-forced

Malwares, spam et fraudes

- BadBIOS: le flop
  - https://twitter.com/dragosr/status/404062382923583488
- … mais les canaux cachés acoustiques, ça peut exister
  - http://www.jocm.us/index.php?m=content&c=index&a=show&catid=124&id=600
- Un malware qui cible Tomcat
  - http://www.symantec.com/connect/blogs/all-your-tomcat-are-belong-bad-guys
- Un malware qui cible SAP
  - http://blogs.technet.com/b/mmpc/archive/2013/11/20/carberp-based-trojan-attacking-sap.aspx
- Une transaction Bitcoin d'environ 150M$
  - https://blockchain.info/tx/1c12443203a48f42cdf7b1acee5b4b1c1fedc144cb909a3bf5edbffafb0cd204
- Quelques malwares à télécharger
  - Android
    - http://contagiominidump.blogspot.fr/
  - Mac OS X
    - http://contagiodump.blogspot.fr/2013/11/osx-malware-and-exploit-collection-100.html

Actualité (francophone)

- **ANSSI**
  - **Guide des bonnes pratiques pour la mise en œuvre d'un système de journalisation**
    - **http://www.ssi.gouv.fr/fr/bonnes-pratiques/recommandations-et-guides/securite-du-poste-de-travail-et-des-serveurs/recommandations-de-securite-pour-la-mise-en-oeuvre-d-un-systeme-de.html**
  - **Sécurité Web #fail ☺**
    - **https://cyh.herokuapp.com/cyh?url=http://www.ssi.gouv.fr**

- **CNIL**
  - **Délibération sur les "coffres-forts numériques"**
    - **http://www.cnil.fr/documentation/deliberations/deliberation/delib/297/**

Actualité (francophone)

- **Fuite de certificat racine au ministère du budget**
  - **L'IGC/A pourrait être retirée des navigateurs**
    - **http://www.reddit.com/r/netsec/comments/1sc3t8/french_ca_anssi_issuing_unauthorized_certs_for/**
    - **http://www.ssi.gouv.fr/fr/menu/actualites/suppression-d-une-branche-de-l-igc-a.html**
    - **http://www.pcinpact.com/news/84830-blocage-certificats-par-google-interview-patrick-pailloux-anssi.htm**
  - **Au passage, l'IGC/A ne respecte pas les exigences applicables aux "root CA" modernes**
    - **Pas de CRL, pas d'OCSP, hash SHA-1, …**
  - **Finalement l'IGC/A ne pourra plus signer que du ".fr"**
    - **http://googleonlinesecurity.blogspot.it/2013/12/further-improving-digital-certificate.html**
  - **Notons qu'il y a au moins un utilisateur de Google Chrome au ministère ☺**
    - **https://code.google.com/p/chromium/codesearch#chromium/src/chrome/browser/net/chrome_fraudulent_certificate_reporter.cc&sq=package:chromium**

Actualité (francophone)

- L'AMF veut réguler Internet
  - http://www.droit-technologie.org/actuality-1623/l-autorite-des-marches-financiers-s-estime-competente-pour-reguler-les.html
- Une législation sur les outils de cybersurveillance
  - Les outils de surveillance à des fins "mercatiques" en sont exemptés ☺
    - http://www.numerama.com/magazine/27730-la-france-encadre-enfin-la-vente-d-outils-de-surveillance-sur-internet.html
- Logiciel Louvois: atterrissage raté
  - http://www.linformaticien.com/actualites/id/31121/louvois-abandonne-qui-va-payer.aspx
- La facture électrique de la DGSE commentée au Sénat
  - http://www.senat.fr/rap/a13-158-5/a13-158-5_mono.html#toc68
- L'école 42 fait sa rentrée

Actualité (francophone)

- Exemple de kit de sensibilisation à la sécurité
  - En milieu hospitalier
    - https://www.sante-centre.fr/portail/espace-d-information/l-actualite-de-la-region/le-portail-sante-centre,72,1526.html
- Renault … la main dans la DRM
    - http://boingboing.net/2013/11/13/renault-ships-a-brickable-car.html
- Imprimer en 3D à la Poste
    - http://www.lemonde.fr/societe/article/2013/11/27/la-poste-se-lance-dans-l-impression-3d_3520839_3224.html
- 149€ le test d'intrusion Web
  - Qui dit mieux ?
    - http://www.testsdintrusion.com/

Actualité (anglo-saxonne)

- **PRISM: une actualité sans fin …**
  - La NSA espionne les sites pornos
    - Pour pouvoir discréditer leurs utilisateurs
      - http://arstechnica.com/tech-policy/2013/11/nsa-spied-on-porn-online-sexual-habits-to-discredit-radicalizers/
  - La NSA effectue 5 milliards de géolocalisations cellulaires … par jour
    - http://www.lemonde.fr/technologies/article/2013/12/04/la-nsa-localise-pres-de-5-milliards-de-portable-par-jour-dans-le-monde_3525520_651865.html
  - Le patron de Belgacom remercié
    - http://www.lemonde.fr/economie/article/2013/11/15/le-patron-de-l-operateur-de-telephonie-belgacom-revoque-par-le-gouvernement_3514855_3234.html
  - Cisco affecté négativement par les conséquences économiques
    - http://qz.com/147313/ciscos-disastrous-quarter-shows-how-nsa-spying-could-freeze-us-companies-out-of-a-trillion-dollar-opportunity/
  - Google et Yahoo! vont chiffrer leurs réseaux internes
    - http://techcrunch.com/2013/11/18/yahoo-will-follow-google-in-encrypting-data-center-traffic-all-traffic-between-company-and-customers-by-q1-14/
  - Bonnes synthèses de l'EFF
    - https://www.eff.org/nsa-spying/nsadocs
    - https://www.eff.org/deeplinks/2013/11/encrypt-web-report-whos-doing-what

Actualité (anglo-saxonne)

- Pas d'iPhone pour Obama
  - … mais il a quand même un iPad ☺
    - http://lexpansion.lexpress.fr/high-tech/pas-d-iphone-pour-obama-pour-des-raisons-de-securite_419053.html#!
- La fin des "patent trolls" ?
    - http://siliconvalley.blog.lemonde.fr/2013/12/06/le-congres-americain-sattaque-aux-patent-trolls-epouvantails-de-la-silicon-valley/
- Comment le FBI cyber-traque des suspects
    - http://www.washingtonpost.com/business/technology/fbis-search-for-mo-suspect-in-bomb-threats-highlights-use-of-malware-for-surveillance/2013/12/06/352ba174-5397-11e3-9e2c-e1d01116fd98_story.html
- La police UK demande des sous aux banques
  - Pour mieux les protéger
    - http://www.scmagazineuk.com/police-banks-pay-to-fight-cybercrime/article/322771

Actualité (européenne)

- **Le guide (Belge) de la cybersécurité**
  - **http://ds.static.rtbf.be/article/pdf/icc_belsec_guide_lr_v2-1385658509.pdf**
- **Google vs. Europe, la saga**
  - **http://www.theregister.co.uk/2013/11/27/google_rivals_oppose_revised_search_business_offer_to_ec/**
- **Les députés européens font de l'ActiveSync sans SSL sur un réseau WiFi ouvert**
  - **http://www.linformaticien.com/actualites/id/31125/des-deputes-europeens-pirates-a-cause-d-une-application-microsoft.aspx**
  - **http://pastebin.com/WR4c2NhJ**

Actualité (Google)

- Faille dans la récupération de mot de passe
  - http://www.orenh.com/2013/11/google-account-recovery-vulnerability.html
- Google vs. CyanogenMod
  - http://www.linformaticien.com/actualites/id/31180/google-n-aime-pas-cyanogenmod.aspx
- Google Takeout
  - Permet de récupérer ses données Gmail et Calendar
    - http://gmailblog.blogspot.fr/2013/12/download-copy-of-your-gmail-and-google.html
- Un compte Google est désormais requis pour télécharger des extensions Chrome
  - http://www.reddit.com/r/privacy/comments/1s5083/chrome_web_store_now_requires_you_to_sign_in_to/

Actualité (Apple)

- **iOS < 7.0.4**
  - **http://support.apple.com/kb/HT6058**

- **Mac OS X < 10.9 sera-t-il encore mis à jour ?**
  - **http://www.zdnet.com/os-x-mountain-lion-users-no-more-security-updates-7000022322/**

Actualité (crypto)

- NTRU devient Open Source (GPL)
  - http://www.net-security.org/secworld.php?id=15997

Actualité

Conférences passées

- GreHack 2013
  - 15 novembre
    - http://grehack.org/
- C&ESAR 2013
  - 19-21 novembre
    - http://www.cesar-conference.org/?page_id=6&lang=fr
    - http://blog.scrt.ch/2013/11/25/csar-2013/
- BotConf 2013
  - 5-6 décembre
    - https://www.botconf.eu/
- PacSec 2013
  - Tout a été cassé au pwn2own (Surface Pro, iPhone 5, Galaxy S4, …)
  - Première victoire d'une équipe chinoise
    - http://www.hppwn2own.com/

Actualité

- **Conférences à venir**
  - **CCC**
    - **https://events.ccc.de/congress/2013/Fahrplan/**
  - **AFCDP**
    - **27 janvier 2014**
      - **http://www.globalsecuritymag.fr/Universite-AFCDP-des-CIL-du-27,20131020,40452.html**
  - **Microsoft TechDays 2014**
    - **11-13 février 2014**
      - **http://www.microsoft.com/france/mstechdays/**
  - **SSTIC 2014**
    - **Soumissions libres !**
      - **https://www.sstic.org/2014/news/CFP_SSTIC_2014/**

Actualité

- **Sorties logicielles**
  - **Metasploit 4.8**
  - **CapStone disassembler**
    - **http://www.capstone-engine.org/**
  - **OfficeMalScanner**
    - **http://www.reconstructer.org/code/OfficeMalScanner.zip**
  - **Obfuscator-LLVM**
    - **https://github.com/obfuscator-llvm/obfuscator/wiki**
  - **MimiLib pour WinDbg**
    - **http://blog.gentilkiwi.com/securite/mimikatz/windbg-extension**
  - **MIDAS**
    - **Outil de sécurité Mac OS X développé par Facebook**
    - **Seul problème: il est naze ☺**
      - **http://www.reddit.com/r/netsec/comments/1sazkn/midas_intrusion_detection_for_macs_by_facebook/**
- **Par contre …**
  - **… c'est fini pour Winamp (au 20 décembre 2013)**

Actualité

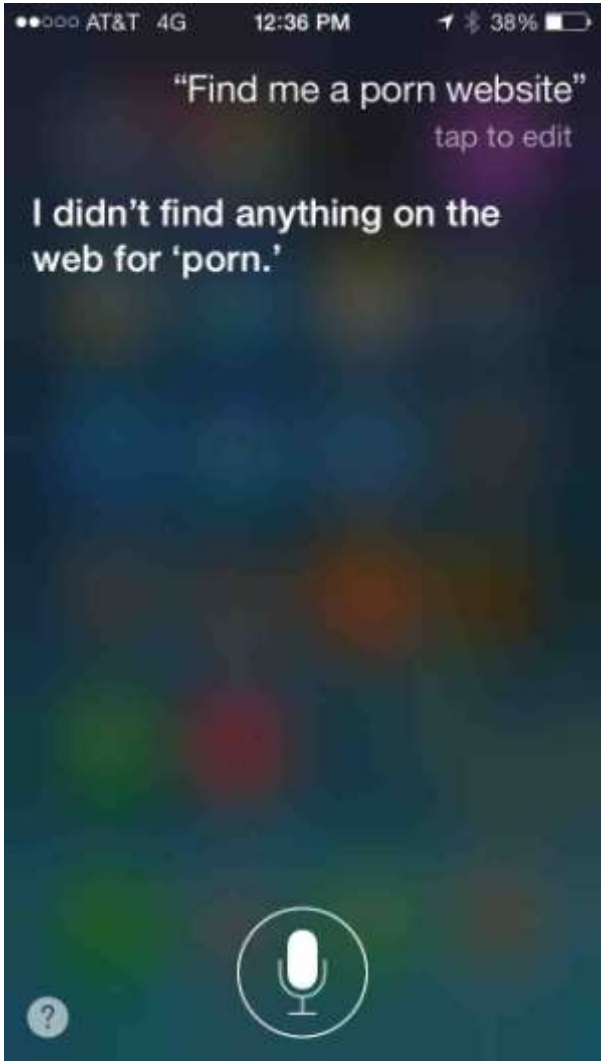
- YotaPhone: le premier smartphone russe
  - http://www.lemonde.fr/technologies/article/2013/12/06/lancement-du-premier-smartphone-made-in-russia_3526642_651865.html#
- Ethos, un système d'exploitation "invulnérable"
  - Avec du D. J. Bernstein dedans
    - http://www.ethos-os.org/
- Le guide du gouvernement japonais contre les APT
  - http://www.ipa.go.jp/files/000035723.pdf

Divers

- Default password #fail
  - http://gizmodo.com/for-20-years-the-nuclear-launch-code-at-us-minuteman-si-1473483587
- Quelle idée de s'appeler "Null" …
  - http://stackoverflow.com/questions/4456438/how-can-i-pass-the-string-null-through-wsdl-soap-from-actionscript-3-to-a-co
- Les licences logicielles présentes dans une voiture
  - http://www4.mercedes-benz.com/manual-cars/ba/foss/content/en/assets/FOSS_licences.pdf
- John Carmack quitte ID Software
  - http://www.giantbomb.com/articles/john-carmack-officially-exits-id-software/1100-4789/

Divers

- **Source**
  - **http://imgur.com/gallery/xwAtrKz**



Divers

- **Source**
  - **https://twitter.com/0xabad1dea/status/407363713440956417/photo/1**

Questions / réponses

- **Questions / réponses**
- **Prochaine réunion et assemblée générale annuelle**
  - **Mardi 14 janvier 2013**
- **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**