OSSIR
Groupe Paris

Réunion du 9 juillet 2013

Revue des dernières vulnérabilités

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

Avis Microsoft

- **Juin 2013**

  - **MS13-047 Correctif cumulatif pour IE (x11) [1]**
    - **Affecte: IE (toutes versions supportées)**
    - **Exploit: corruption mémoire (x19)**
    - **Crédits:**
      - **Scott Bell / Security-Assessment.com**
      - **SkyLined + ZDI (x2)**
      - **anonymous + ZDI (x4)**
      - **Ivan Fratric & Ben Hawkes / Google Security Team (x4)**
      - **Omair + ZDI**
      - **Stephen Fewer of Harmony Security + ZDI**
      - **Aniway.Anyway@gmail.com + ZDI (x2)**
      - **Amol Naik and Omair + ZDI (x2)**
      - **Toan Pham Van + ZDI**

  - **MS13-048 Fuite d'information dans le noyau Windows (x1) [3]**
    - **Affecte: Windows (toutes versions 32 bits)**
    - **Exploit: fuite d'information**
    - **Crédits: Mateusz "j00ru" Jurczyk / Google Inc**

Avis Microsoft

- **MS13-049 Faille dans la pile TCP/IP (x1) [3]**
  - **Affecte: Windows (toutes versions supportées, sauf XP/2003)**
  - **Exploit: déni de service distant**
  - **Crédits: n/d**

- **MS13-050 Elévation de privilèges dans Print Spooler (x1) [1]**
  - **Affecte: Windows (toutes versions supportées, sauf XP/2003)**
  - **Exploit: élévation de privilèges lors de la suppression d'une imprimante**
  - **Crédits: n/d**

Avis Microsoft

- MS13-051 Faille dans le support PNG (x1) [1]
  - Affecte: Office 2003 SP3, Office 2011 pour Mac
  - Exploit: exécution de code à l'ouverture d'un document malformé
    - Utilisé dans des "attaques ciblées"
  - Crédits: Andrew Lyons & Neel Mehta / Google Inc

Avis Microsoft

- **Advisories**

  - **Q2719662**
    - **V1.1: désactiver les gadgets permet de se protéger contre la faille**
  - **Q2755801**
    - **V13.0: mise à jour du Flash Player intégré à IE10**
  - **Q2854544**
    - **V1.0: gestion centralisée des CTL**

Avis Microsoft

- **Prévisions pour Juillet 2013**
  - **7 bulletins (6 critiques, 1 important)**
  - **Windows, IE, .NET, composants partagés, Windows Defender, …**
- **Failles à venir**
- **Retour sur des failles antérieures**

Avis Microsoft

- **Révisions**
  - **MS12-006**
    - **V1.3: correction documentaire**
  - **MS12-052**
    - **V1.2: ajout d'un problème connu**
  - **MS12-069**
    - **V1.1: correction documentaire**
  - **MS12-079**
    - **V1.1: ajout d'un problème connu**
  - **MS13-029**
    - **V2.0: republication du bulletin pour RDP 7.0 sur Windows XP SP3**
  - **MS13-038**
    - **V1.1: ajout d'un problème connu**
  - **MS13-040**
    - **V1.1: liste de plateformes sur lesquelles .NET Framework ne peut pas être installé**
  - **MS13-048**
    - **V1.1: ajout d'un problème connu**
    - **V1.2: changement dans la logique de détection**

Infos Microsoft

Sorties logicielles

- Office sur iPhone/iPad
  - Uniquement pour les abonnés Office 365
- "Preview"
  - Visual Studio 2013
  - .NET 4.5.1
  - Windows 2012 R2
  - System Center 2012 R2
  - …
- SQL Server 2014 CTP1

Infos Microsoft

Autre

- **Microsoft lance un Bug Bounty !**
  - **http://www.microsoft.com/security/msrc/report/bountyprograms.aspx**
  - **$150,000 pour Windows 8.1**
  - **$500 à $11,000 pour IE11**
    - **http://www.microsoft.com/security/msrc/report/IE11.aspx**

- **Concours Azure**
  - **Une Aston Martin à gagner**
    - **http://azuremsdnsweepstakes.azurewebsites.net/8675309_rules.aspx**

- **Microsoft + Oracle =**
  - **Java, Oracle DB, Linux, WebLogic sur Azure et Windows Server**

- **Les abonnements TechNet disparaissent**
  - **http://technet.microsoft.com/subscriptions/ms772427**

- **Démantèlement du botnet "Citadel"**
  - **http://www.microsoft.com/en-us/news/Press/2013/Jun13/06-05DCUPR.aspx**

Infos Réseau

- **(Principales) faille(s)**
  - **Failles Cisco**
    - http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130626-ngfw
    - http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130626-sma
    - http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130626-wsa
    - http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130626-esa
    - http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130619-tpc
    - …
  - **Faille dans le serveur Web embarqué dans les routeurs Huawei**
    - "Heap overflow" quand la taille des données HTTP != "Content-Length" ☺
      - http://www.huawei.com/en/security/psirt/security-bulletins/security-advisories/hw-u_194361.htm
  - **Faille (triviale) SolusVM**
    - De nombreux hébergeurs attaqués
      - http://www.reddit.com/r/netsec/comments/1giquf/solusvm_0day_used_on_major_vps_hosts/caksxdt
  - **BIND 9**
    - Déni de service
      - https://kb.isc.org/article/AA-00967/0/CVE-2013-3919%3A-A-recursive-resolver-can-be-crashed-by-a-query-for-a-malformed-zone.html

Infos Réseau

- **Autres infos**

  - **L'ICANN veut centraliser le WHOIS**
    - **http://www.computerworld.com.au/article/465895/icann_working_group_seeks_kill_whois/**

  - **La différence entre DPI et antispam ?**
    - **http://www.numerama.com/magazine/26297-ovh-copie-et-analyse-tous-les-e-mails-sortant-de-ses-serveurs.html**

Infos Unix

- (Principales) faille(s)
  - Faille dans le support ext4 sous Linux
    - http://forums.grsecurity.net/viewtopic.php?f=3&t=3574

Infos Unix

- **Autres infos**
  - **Un repo Debian devient "non officiel"**
    - **http://bits.debian.org/2013/06/remove-debian-multimedia.html**
  - **Hurray!**
    - **Debian supporte GNU/Hurd comme noyau**
      - **http://lwn.net/Articles/554992/**

Failles

- **Principales applications**
  - **Adobe Flash Player**
    - **http://www.adobe.com/support/security/bulletins/apsb13-16.html**
  - **Java < 1.7.25**
    - **40 failles**
      - **http://www.oracle.com/technetwork/topics/security/javacpujun2013-1899847.html**
    - **Le mise à jour pour Mac OS X est disponible**
      - **http://support.apple.com/kb/HT5797?viewlocale=fr_FR**
  - **Patch trimestriel Oracle**
    - **Prévu pour le 16 juillet**
      - **http://www.oracle.com/technetwork/topics/security/alerts-086861.html**
  - **Firefox < 22.0**
  - **Thunderbird < 17.0.7**
  - **Chrome**
    - **http://googlechromereleases.blogspot.fr**
    - **https://sites.google.com/a/chromium.org/dev/Home/chromium-security**
  - **VLC < 2.0.7**

Failles

- Injection SQL "pre auth" dans McAfee ePO
  - http://funoverip.net/2013/06/mcafee-epolicy-0wner-preview/
- "Stack overflow" exploitable à distance dans Symantec EPM
  - http://www.symantec.com/security_response/securityupdates/detail.jsp?fid=security_advisory&pvid=security_advisory&year=&suid=20130618_00
- Apple Mac OS 10.6.x Directory Service
  - http://www.coresecurity.com/advisories/mac-osx-server-directoryservice-buffer-overflow
- Backdoor dans HP StoreOnce
  - HPSupport / badg3r5
    - http://www.lolware.net/hpstorage.html
- Contournement de l'authentification dans HP iLO
  - http://www.certa.ssi.gouv.fr/site/CERTA-2013-AVI-372/CERTA-2013-AVI-372.html

Failles 2.0

- **Contournement de la signature des fichiers APK**
  - **A venir lors de BH US 2013**
    - **http://bluebox.com/corporate-blog/bluebox-uncovers-android-master-key/**

Sites piratés

- Campagnes APT
  - "Naikon"
    - http://www.trendmicro.co.id/id/news/news_20130613_2.html
  - "NetTraveler"
    - http://www.prnewswire.com/news-releases/kaspersky-lab-uncovers-operation-nettraveler-a-global-cyberespionage-campaign-targeting-government-affiliated-organisations-and-research-institutes-210808801.html

- Les sites piratés du mois (liste partielle)
  - Opera: "*security breach stopped*"
    - Les certificats de signature visés
      - http://my.opera.com/securitygroup/blog/2013/06/26/opera-infrastructure-attack
    - Un malware déjà signé avec ce certificat
      - http://blog.trendmicro.com/trendlabs-security-intelligence/spyware-hides-behind-stolen-opera-digital-certificate/
  - Ubisoft Uplay
    - https://support.ubi.com/en-US/FAQ.aspx?platformid=60&productid=3888&faqid=kA030000000eYZ2CAM
  - Facebook
    - 6M de comptes
      - http://www.theregister.co.uk/2013/06/21/facebook_contact_leak/
  - Le compte Twitter d'Auchan
    - http://www.numerama.com/magazine/26238-auchan-se-fait-pirater-son-compte-twitter.html

Malwares, spam et fraudes

- Les premières "erreurs de paiement" liées aux cartes sans contact
  - http://www.bbc.co.uk/news/business-22545804
- L'authentification à 2 facteurs gagne du terrain
  - LinkedIn (après Google, Facebook, Apple, Twitter …)
    - http://blog.linkedin.com/2013/05/31/protecting-your-linkedin-account-with-two-step-verification/
- Taux de mise à jour Java
  - 93% des utilisateurs sont vulnérables
    - http://community.websense.com/blogs/securitylabs/archive/2013/06/04/majority-of-users-still-vulnerable-to-java-exploits.aspx
- Attaquer un téléphone Android
  - … via le signal RDS !
    - http://ieeexplore.ieee.org/xpl/abstractAuthors.jsp?arnumber=6507551

Malwares, spam et fraudes

- Le code source de Carberp dans la nature
- 5 pirates français arrêtés
  - 27,000 comptes bancaires détournés, $9m de butin
    - http://www.linformaticien.com/actualites/id/29388/piratage-coup-de-filet-sur-5-cybercriminels-francais.aspx
- Compromission massive en Corée du Sud
  - A cause du processus de mise à jour automatique du logiciel SimDisk
    - http://blog.trendmicro.com/trendlabs-security-intelligence/compromised-auto-update-mechanism-affects-south-korean-users/
- Une instruction FPU non documentée pour contourner les émulateurs
    - http://blogs.technet.com/b/mmpc/archive/2013/06/24/investigation-of-a-new-undocumented-instruction-trick.aspx
  - Ou pas
    - http://web.archive.org/web/19970411042924/http://www.sandpile.org/80x86/opc_fpu.shtml

Actualité (francophone)

- **Publications ANSSI**
  - **PASSI 1.0**
    - **http://www.ssi.gouv.fr/fr/menu/actualites/publication-du-referentiel-d-exigences-applicable-aux-prestataires-d-audit-de.html**
  - **Le guide du PCA**
    - **http://www.sgdsn.gouv.fr/IMG/pdf/Guide_PCA_SGDSN_120613_web.pdf**
- **Certifications CSPN**
  - **http://www.ssi.gouv.fr/fr/produits-et-prestataires/produits-certifies-cspn/**
    - **2013/07 rWeb 4.1 FP1 (Deny-All)**
    - **2013/06 Teopad (Thales)**
    - **2013/05 Dropbear**

Actualité (francophone)

- "Chorus" en panne
  - Note: c'est du Cloud français hébergé chez Bull ☺
    - http://www.lesechos.fr/entreprises-secteurs/tech-medias/actu/0202846131025-bercy-victime-d-une-panne-de-son-logiciel-de-comptabilite-578450.php
- Big Brother Awards
    - http://bigbrotherawards.eu.org/
- HADOPI: première "suspension" d'Internet !
  - Ou pas
    - http://www.linformaticien.com/actualites/id/29383/hadopi-premiere-suspension-d-acces-web-ordonnee.aspx
- "Cyberdéfense as a Service"
    - http://www.silicon.fr/cyberdefense-as-a-service-atheos-87516.html

Actualité (francophone)

- La sécurité physique peut aussi être un échec
  - http://www.letelegramme.fr/ig/generales/fait-du-jour/ile-longue-des-failles-dans-la-securite-11-06-2013-2132250.php
  - http://www.letelegramme.fr/ig/generales/regions/bretagne/ile-longue-la-base-ses-recoins-ses-personnages-cles-12-06-2013-2130828.php
  - …

Actualité (anglo-saxonne)

- La CIA publie un mémo disant d'arrêter les fuites
  - Problème: le mémo a fuité ☺
    - http://bigstory.ap.org/article/cia-cracks-down-its-own-stop-leaks

Actualité (européenne)

- La législation contre les cybercriminels se durcit
  - (Est-ce une bonne chose sachant qu'ils sont pour la plupart non-européens ?)
    - http://www.europarl.europa.eu/news/fr/pressroom/content/20130701IPR14763/html/Cyber-attaques-le-Parlement-adopte-des-sanctions-communes-plus-strictes
- Les pouvoirs de l'ENISA se renforcent
    - https://www.enisa.europa.eu/media/press-releases/nouvelle-directive-de-l2019enisa-l-agence-europeenne-chargee-de-la-securite-des-reseaux-et-de-l2019information-les-nouvelles-fonctions-de-l2019agence
- L'Europe cherche des experts juridiques du Cloud
    - http://europa.eu/rapid/press-release_IP-13-590_fr.htm

Actualité (Google)

- Google migre tous ses certificats vers RSA-2048+ …
  - … et active "Server Name Indication" sur TLS
  - Petit détail: aucune version d'IE sur Windows XP n'est compatible
    - http://nakedsecurity.sophos.com/2013/06/05/google-certificate-announcement/
- Une analyse anti-malware sur Google Web Store
    - https://plus.google.com/+GoogleChromeDevelopers/posts/3kpAu4VcP5E
- Google Loon
  - Des dirigeables pour l'Internet
    - http://www.google.com/loon/
- CNIL vs. Google
    - http://www.cnil.fr/linstitution/actualite/article/article/la-cnil-met-en-demeure-google-de-se-conformer-dans-un-delai-de-trois-mois-a-la-loi-informatique/

Actualité (Apple)

- Le président de YSL recruté par Apple

Actualité (crypto)

- Ca chauffe pour la résolution du logarithme discret sur courbes elliptiques
  - http://ellipticnews.wordpress.com/2013/06/21/quasi-polynomial-time-algorithm-for-discrete-logarithm-in-finite-fields-of-smallmedium-characteristic/
- La NSA propose de nouveaux algorithmes symétriques
  - SIMON et SPECK
    - http://www.schneier.com/blog/archives/2013/07/simon_and_speck.html
- La crypto homomorphique avance
  - http://web.mit.edu/newsoffice/2013/algorithm-solves-homomorphic-encryption-problem-0610.html
- Note pour plus tard: ne pas utiliser e=1 ☺
  - https://github.com/saltstack/salt/commit/5dd304276ba5745ec21fc1e6686a0b28da29e6fc

Actualité

- **Conférences passées**
  - **Hack In Paris 2013 / Nuit du Hack**
    - **https://www.hackinparis.com/talk**
  - **Recon 2013**
    - **http://www.recon.cx/2013/schedule/schedule.html**

- **Conférences à venir**
  - **OHM**
  - **Hack.Lu 2013**
  - **GreHack 2013**
  - **BotConf**

Actualité

- Sorties logicielles

Actualité

- **PRISM (et assimilés)**
  - **Source initiale**
    - **http://www.guardian.co.uk/world/2013/jun/06/us-tech-giants-nsa-data**
  - **Réactions**
    - **http://gigaom.com/2013/07/04/france-has-its-own-prism-like-surveillance-program-report-suggests/**
    - **http://www.guardian.co.uk/uk/2013/jun/21/gchq-mastering-the-internet**
    - **http://french.china.org.cn/foreign/txt/2013-06/17/content_29143053.htm**
    - **http://china.org.cn/world/2013-06/20/content_29176541.htm**
    - **http://www.lesechos.fr/entreprises-secteurs/tech-medias/actu/0202845256760-prism-la-nsa-a-recrute-l-ancien-chef-de-la-securite-informatique-de-facebook-578334.php**
    - **https://prism-break.org/**
    - **…**

Actualité

- Entre les deux
  - http://www.wnd.com/2013/06/nsa-has-total-access-via-microsoft-windows/
  - …
- Fun
  - http://vidberg.blog.lemonde.fr/files/2013/06/161_surveillance.gif
  - http://www.slideshare.net/EmilandDC/dear-nsa-let-me-take-care-ou
  - http://www.legorafi.fr/2013/06/07/la-nsa-sengage-a-nettoyer-les-spams-des-boites-mail-quelle-surveille/
  - http://prism.andrevv.com/
  - …

- Une seule leçon: on ne se méfie jamais assez de son sysadmin

Actualité

- **VISA et MasterCard ne travaillent plus avec les fournisseurs de VPN anonymisant**
  - **https://www.techdirt.com/articles/20130703/13150923710/visa-mastercard-ban-anonymizing-vpns-just-as-they-allow-wikileaks.shtml**

- **Benchmark de 12 solutions eCommerce**
  - **http://www.nbs-system.co.uk/blog/benchmark-of-e-commerce-solutions.html**

Divers

- Jeu vidéo .. ou réalité ?
  - Les deux !
    - http://wearedata.watchdogs.com/
- Yahoo!
  - … rachète QWiki
  - … ferme AltaVista (et d'autres)
    - http://techcrunch.com/2013/06/28/yahoo-to-sunset-alta-vista-axis-rss-alerts-and-nine-other-products-some-as-soon-as-today/
- Le 28 juin c'était la journée du CAPS LOCK
  - Prochaine le 22 octobre
    - http://www.pcinpact.com/news/80898-aujourdhui-cest-la-journee-du-caps-lock.htm
- A priori, on devrait tous être en train de mourir
    - http://www.lepoint.fr/science/un-trou-dans-le-soleil-menace-les-communications-en-europe-de-l-ouest-12-06-2013-1679867_25.php

Divers

- Michael Birch rachète Bebo.com pour $1m
  - Après l'avoir vendu $850m à AOL
    - http://www.businessinsider.com/michael-birch-buys-bebo-back-for-1-million-2013-7
- "Only CISSPs can defend against The APT"
    - http://www.aptdefender.com/index.html
- Javapocalypse
    - http://www.youtube.com/watch?v=E3418SeWZfQ
- John McAfee lui-même
  - … vous aide à désinstaller McAfee
    - http://www.youtube.com/watch?v=bKgf5PaBzyg

Questions / réponses

- **Questions / réponses**
- **Prochaine réunion**
  - **Mardi 10 septembre 2013**
- **Bonnes vacances à tous !**