OSSIR
Groupe Paris

Réunion du 5 avril 2011

Revue des dernières vulnérabilités

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

Avis Microsoft

- **Février 2011**
  - **12 bulletins, dont 3 critiques**
    - **22 failles**
    - **Windows, Internet Explorer, Office, Visual Studio, IIS (FTP sur 7.0 et 7.5)**
    - **Q2490606 (support des miniatures) et Q2488013 (IE)**
  - **Références**
    - **http://blogs.technet.com/b/msrc/archive/2011/02/08/february-2011-security-bulletin-release.aspx**
    - **http://blogs.technet.com/b/srd/archive/2011/02/08/assessing-the-risk-of-the-february-security-updates.aspx**
    - **http://blogs.technet.com/b/msrc/p/february-2011-security-bulletin-q-a.aspx**
  - **MS11-003 Correctif cumulatif pour Internet Explorer [1,1,1]**
    - **Affecte: Internet Explorer (toutes versions supportées)**
    - **Exploit: 4 failles dont certaines exploitées dans la nature**
    - **Crédit:**
      - **Yuki Chen / Trend Micro**
      - **SkyLined / Google**
      - **Haifei Li / Fortinet**

Avis Microsoft

- MS11-004 Faille dans le serveur FTP [1]
  - Affecte: IIS 7.0 et 7.5
  - Exploit: exploité dans la nature
    - http://blogs.technet.com/b/srd/archive/2011/02/08/regarding-ms11-004-addressing-an-iis-ftp-services-vulnerability.aspx
  - Crédit: n/d

- MS11-005 Déni de service sur Active Directory [3]
  - Affecte: Windows 2003
  - Exploit: collision possible sur le SPN, forçant un *downgrade* en NTLM
  - Crédit: n/d

Avis Microsoft

- MS11-006 Faille dans le support des miniatures [1]
  - Affecte: Windows (toutes versions supportées, sauf Seven et 2008R2)
  - Exploit: exploité dans la nature
    - http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=890
  - Crédit: Kobi Pariente & Yaniv Miron / iDefense
  - Note: incompatibilité avec le client VMWare View

- MS11-007 Faille dans le support OpenType CFF [1]
  - Affecte: Windows (toutes versions supportées)
  - Exploit: élévation de privilèges utilisateur vers noyau
    - Exploitable depuis une page Web avec Windows Vista, 2008, Seven, 2008R2
  - Crédit: n/d

Avis Microsoft

- MS11-008 Failles dans Visio [1,1]
  - Affecte: Visio 2002, 2003 et 2007 (sauf Viewer)
  - Exploit: exécution de code à l'ouverture d'un fichier Visio malformé
  - Crédit:
    - Procyun / ZDI-11-063
    - Xin Ouyang / Palo Alto Networks (x2)

- MS11-009 Faille dans JScript et VBScript [3]
  - Affecte: Windows Seven et 2008R2
  - Exploit: fuite d'information sur la mémoire
  - Crédit: Yamata Li / Palo Alto Networks

Avis Microsoft

- MS11-010 Faille dans CSRSS [1]
  - Affecte: Windows XP et 2003
  - Exploit: il est possible de continuer à exécuter du code après la fermeture de session
  - Crédit:
    - Sihan Qing (Professor)
    - Weiping Wen (Associate Professor)
    - Liang Yi & Husheng Zhou (Graduate students)
    - / Department of Information Security, Beijing University

- MS11-011 Faille noyau [1]
  - Affecte: Windows (toutes versions supportées)
  - Exploit: élévation de privilèges
  - Crédit:
    - Zhengwenbin / 360safe
    - Guo Bojun
    - Wei Zhang
    - Marco Giuliani / Prevx
    - std_logic / ZDI-11-064

Avis Microsoft

- **MS11-012 Failles dans WIN32K [1,1,1,1,1]**
  - **Affecte: Windows (toutes versions supportées)**
  - **Exploit: élévation de privilèges utilisateur vers noyau**
  - **Crédit: Tarjei Mandt / Norman (x5)**

- **MS11-013 Faille dans Kerberos [1,1]**
  - **Affecte: Windows (toutes versions supportées, sauf Vista et 2008)**
  - **Exploit: élévation de privilèges**
    - **Utilisation d'algorithmes de hash au lieu de HMAC**
    - ***Downgrade* possible vers DES**
  - **Crédit:**
    - **MIT Kerberos Team**
    - **Scott Stender / iSEC Partners**

Avis Microsoft

- **MS11-014 Faille dans LSASS [1]**
  - **Affecte: Windows XP et 2003**
  - **Exploit: élévation de privilèges locale**
  - **Crédit: Jorge Moura / Primavera BSS**

Avis Microsoft

- **Mars 2011**
  - **3 bulletins, 4 failles**
  - **Références**
    - **n/a**
  - **MS11-015 Failles dans Windows Media [1,1]**
    - **Affecte: Windows XP SP3, Vista (toutes versions), Windows 7 (toutes versions), Windows 2008 R2 (Gold/SP1)**
    - **Exploit:**
      - **"*DLL Preloading*" dans DirectShow**
      - **Exécution de code à l'ouverture d'un fichier ".dvr-ms" malformé**
    - **Crédit:**
      - **Matthew Watchinski / SourceFire VRT**

Avis Microsoft

- **MS11-016 Faille dans Microsoft Groove [1]**
  - **Affecte: Microsoft Groove 2007 SP2 (uniquement)**
  - **Exploit: "*DLL Preloading*"**
  - **Crédit: H.D.Moore / Rapid7**

- **MS11-017 Faille dans Remote Desktop [1]**
  - **Affecte: client Remote Desktop 5.2 - 7.0**
  - **Exploit: "*DLL Preloading*"**
  - **Crédit: Eyal Gruner / Versafe Anti Fraud**

Avis Microsoft

- **Prévisions Microsoft pour avril**
  - **n/d**

- **Advisories**

  - **Q967940 Désactivation de l'AutoRun/AutoPlay**
    - **V2.0: cette mise à jour est offerte à tous les utilisateurs**
      - **http://blogs.technet.com/b/mmpc/archive/2011/02/08/breaking-up-the-romance-between-malware-and-autorun.aspx**
      - **http://blogs.technet.com/b/msrc/archive/2011/02/08/deeper-insight-into-the-security-advisory-967940-update.aspx**
    - **V2.1: changement dans la logique de détection**

  - **Q973811 "Extended Protection for Authentication"**
    - **V1.12: <TODO>**

  - **Q2269637 "DLL Preloading"**
    - **V5.0: publication du bulletin MS11-003 pour IE**
    - **V6.0: publication des bulletins MS11-015, MS11-016 et MS11-017**

Avis Microsoft

- **Q2488013 Faille dans les feuilles de style sous IE**
  - **V2.0: publication du bulletin**
- **Q2490606 Faille dans le support des miniatures**
  - **V2.0: publication du bulletin**
- **Q2501696 XSS générique au travers du protocole mhtml://**
  - **V1.0: avis publié**
  - **V1.1: attaques ciblées exploitant cette faille**

Avis Microsoft

- Q2491888 Elévation de privilèges dans Microsoft Malware Protection Engine
  - V1.0: avis publié
  - V1.1: ForeFront pour Exchange n'est pas affecté
- Q<TODO> Elévation de privilèges dans le service d'optimisation .NET
  - Le binaire peut être modifié par tout utilisateur de domaine !
    - http://www.exploit-db.com/exploits/16940/
- Q2524375 Emission de certificats frauduleux
  - On y reviendra …
- Q2508823 Mise à jour pour le client ForeFront
  - Si le correctif échoue à s'installer, le client ForeFront est désinstallé complètement
    - http://blogs.technet.com/b/clientsecurity/archive/2011/03/08/fcs-v1-march-2011-update.aspx

Avis Microsoft

- **Révisions**
  - **MS10-070**
    - **V4.0: changement dans la logique de détection**
      - **Suite à Windows Seven SP1**
  - **MS10-077**
    - **V3.0: changement dans la logique de détection**
      - **Suite à Windows Seven SP1**
  - **MS11-003**
    - **V2.0: Windows Seven SP1 / 2008R2 SP1 sont aussi affectés**
  - **MS11-004**
    - **V2.0: Windows Seven SP1 / 2008R2 SP1 sont aussi affectés**
  - **MS11-006**
    - **V1.1: le *workaround* doit être annulé avant l'installation du correctif**

Avis Microsoft

- MS11-007
  - V2.0: Windows Seven SP1 / 2008R2 SP1 sont aussi affectés
- MS11-009
  - V2.0: Windows Seven SP1 / 2008R2 SP1 sont aussi affectés
- MS11-011
  - V1.2: Windows Seven SP1 / 2008R2 SP1 ne sont pas affectés
- MS11-012
  - V2.0: Windows Seven SP1 / 2008R2 SP1 sont aussi affectés
- MS11-013
  - V2.0: Windows Seven SP1 / 2008R2 SP1 sont aussi affectés
- MS11-015
  - V1.1: corrections documentaires dans la table de support SMS
  - V1.2: Windows XP Home et Tablet sont affectés
- MS11-017
  - V1.1: corrections documentaires dans la table de support SMS
  - V1.2: Remote Desktop 7.1 n'est pas affecté

Infos Microsoft

- Sorties logicielles
  - Windows Seven / 2008R2 SP1
    - Parmi les nouveautés
      - "Dynamic Memory" pour Hyper-V
      - RemoteFX (RDP accéléré)
      - … et surtout plein de *bugfixes* !
      - http://technet.microsoft.com/en-us/library/ff817622%28WS.10%29.aspx
  - Internet Explorer 9
  - Visual Studio 2010 SP1
  - SQL Server 2005 SP4

Infos Microsoft

- **Autre**
  - **Déni de service sur les contrôleurs de domaine Windows 2003 (0day)**
    - **http://archives.neohapsis.com/archives/fulldisclosure/2011-02/0284.html**
    - **http://blogs.technet.com/b/srd/archive/2011/02/16/notes-on-exploitability-of-the-recent-windows-browser-protocol-issue.aspx**
  - **ZDI commence à publier les failles qui ont dépassé les 180 jours !**
    - **Failles Excel**
      - **ZDI-11-040, ZDI-11-041, ZDI-11-042, ZDI-11-043**
    - **Faille PowerPoint**
      - **ZDI-11-044**
  - **SDL vs. PCI DSS**
    - **http://blogs.msdn.com/b/sdl/archive/2011/02/11/sdl-and-pci-dss-pa-dss-aligning-security-practices-and-compliance-activities.aspx**
  - **Scrum Day**
    - **Le 31 mars chez Microsoft**
      - **http://www.scrumday.fr/**

Infos Microsoft

- **Bloquer le port FireWire sur Windows**
  - **http://support.microsoft.com/kb/2516445**
- **La fin d'IE6 (ou pas)**
  - **http://www.ie6countdown.com/**
- **Windows Phone 7 devient le système principal de Nokia**
  - **Montant du *deal*: $1 milliard**
- **Microsoft arrête le Zune**
  - **http://www.linformaticien.com/actualites/id/10556/microsoft-arrete-le-zune.aspx**
- **Un cadre de Microsoft passe chez Salesforce avec 600 Mo de données confidentielles**
  - **http://www.solutions-logiciels.com/actualites.php?actu=9040**

Infos Réseau

- (Principales) faille(s)
  - Cisco ASA
    - 4 failles dont 3 "dénis de service" (IPv6, SCCP, RIP)
      - http://www.cisco.com/warp/public/707/cisco-sa-20110223-asa.shtml
  - Cisco FWSM (FireWall Service Module)
    - "Déni de service" dans le support du protocole SCCP
      - http://www.cisco.com/warp/public/707/cisco-sa-20110223-fwsm.shtml
  - Cisco Téléprésence
    - Failles multiples (graves voire critiques)
      - http://www.cisco.com/warp/public/707/cisco-sa-20110223-telepresence-cts.shtml
      - http://www.cisco.com/warp/public/707/cisco-sa-20110223-telepresence-ctsman.shtml
      - http://www.cisco.com/warp/public/707/cisco-sa-20110223-telepresence-ctms.shtml
      - http://www.cisco.com/warp/public/707/cisco-sa-20110223-telepresence-ctrs.shtml
  - Cisco Linksys WAP610N
    - Accès root sans authentification sur le port TCP/1111
      - http://www.securenetwork.it/ricerca/advisory/download/SN-2010-08.txt

Infos Réseau

- **Probablement les pires failles depuis que Cisco publie des bulletins:**
  - **Cisco ACS**
    - **http://www.cisco.com/warp/public/707/cisco-sa-20110330-acs.shtml**
  - **Cisco NAC**
    - **http://www.cisco.com/warp/public/707/cisco-sa-20110330-nac.shtml**
- **Le reste des avis Cisco est décalé du 23 mars … au 28 septembre**
    - **http://seclists.org/bugtraq/2011/Mar/170**

Infos Réseau

- BIND < 9.7.3
  - Déni de service via IXFR
    - http://www.isc.org/software/bind/advisories/cve-2011-0414
- MIT Kerberos 5
    - http://web.mit.edu/kerberos/advisories/MITKRB5-SA-2011-001.txt
    - http://web.mit.edu/kerberos/advisories/MITKRB5-SA-2011-002.txt
  - PKINIT
    - http://web.mit.edu/kerberos/advisories/MITKRB5-SA-2011-003.txt
- Quagga < 0.99.18
  - Déni de service
    - http://www.quagga.net/news2.php?y=2011&m=3&d=21#id1300723200
- Avahi < 0.6.29
  - Déni de service … avec un paquet vide
    - http://www.avahi.org/ticket/325

Infos Réseau

- Postfix
  - Injection de commandes SMTP avant le STARTTLS
    - http://www.postfix.org/announcements/postfix-2.7.3.html
- Pure-FTPd < 1.0.30
  - … aussi
    - http://www.pureftpd.org/project/pure-ftpd/news
- ProFTPd
  - Déni de service via S/FTP
    - http://bugs.proftpd.org/show_bug.cgi?id=3586
- Client rsync < 3.0.8
  - Exploitable par un serveur malveillant
    - http://rsync.samba.org/ftp/rsync/src/rsync-3.0.8-NEWS
- Samba
  - Déni de service
    - http://samba.org/samba/security/CVE-2011-0719.html

Infos Réseau

- Autres infos
  - IPv4, la spéculation commence ?
    - http://www.linformaticien.com/Actualit%C3%A9s/tabid/58/newsid496/10638/microsoft-7-5-millions-pour-666-624-adresses-ipv4/Default.aspx
  - uTorrent collecte des informations sur ses utilisateurs
    - Pour effectuer une comparaison mondiale des ISP ?
      - http://www.hackinthebox.org/index.php?name=News&file=article&sid=40153
  - ComCast FAIL
    - Mot de passe "en dur" dans leur modem
      - mso / D0nt4g3tme
      - https://www.trustwave.com/spiderlabs/advisories/TWSL2011-002.txt

Infos Réseau

- Le domaine "sun.com" va disparaitre le 1er juin
  - L'un des 100 premiers domaines à avoir existé
    - http://www.linformaticien.com/actualites/id/10571/sun-com-va-disparaitre.aspx
- NANOG devient NewNOG
    - http://www.merit.edu/news/newsarchive/article.php?article=20110201_nanog
- Le ".42", un TLD associatif
    - https://www.42registry.org/

Infos Unix

- (Principales) faille(s)
  - Noyau Linux
    - Elévation de privilèges locale (sans correctif)
      - CVE-2011-1011
        - http://archives.neohapsis.com/archives/fulldisclosure/2011-02/0585.html
      - CVE-2011-1012
        - Exécution de code au montage d'une partition
  - GNU Libc: fnmatch()
    - Ulrich Drepper se fait encore remarquer …
      - http://scarybeastsecurity.blogspot.com/2011/02/i-got-accidental-code-execution-via.html
  - OpenSSL < 1.0.0d, < 0.9.8r
    - Déni de service
    - Exploitable dans Apache (entre autres)
      - http://www.openssl.org/news/secadv_20110208.txt

Infos Unix

- Injection de commandes dans la variable d'environnement locale par la libc
  - Entre autres …
    - http://rhn.redhat.com/errata/RHSA-2011-0412.html
- LibTIFF 3.9.4
  - Un impact potentiellement énorme
    - CVE-2011-0192
- Oracle 10 sur Solaris
  - Le fichier "undo.Z", accessible en lecture, contient les hashes des mots de passe Oracle ainsi que celui de root
    - CVE-2011-412
- Ruby
    - http://www.ruby-lang.org/en/news/2011/02/18/fileutils-is-vulnerable-to-symlink-race-attacks/
    - http://www.ruby-lang.org/en/news/2011/02/18/exception-methods-can-bypass-safe/

Infos Unix

- PHP < 5.3.6
  - Failles multiples …
    - http://www.php.net/archive/2011.php#id2011-03-17-1
- Zend Server Java Bridge 3.1
  - Exécution de code Java sur le port TCP/10001
    - http://www.zend.com/en/products/server/updates

Infos Unix

- phpMyAdmin
  - Un bookmark permet de faire exécuter du code SQL à un autre utilisateur
    - http://www.phpmyadmin.net/home_page/security/PMASA-2011-2.php
- WordPress < 3.0.5
    - http://wordpress.org/news/2011/02/wordpress-3-0-5/
- WordPress < 3.1.1
    - http://wordpress.org/news/2011/04/wordpress-3-1-1/
- MediaWiki < 1.16.2
  - XSS
- Dokeos < 1.8.6.2
  - Lecture de fichiers arbitraires …
    - http://dokeos.com/en/node/892

Infos Unix

- Django
  - Failles multiples
    - http://www.djangoproject.com/weblog/2011/feb/08/security/
- Ruby on Rails
  - XSS, contournement des filtres sur un système de fichiers insensible à la casse, injection SQL dans la méthode limit()
    - http://weblog.rubyonrails.org/2011/2/8/new-releases-2-3-11-and-3-0-4
- WebSphere
  - Fuite d'informations
    - http://www-01.ibm.com/support/docview.wss?uid=swg21460422
- Apache Tomcat < 5.5.32, < 6.0.32, < 7.0.8
  - XSS, déni de service …

Infos Unix

- **Joomla! <= 1.5.22**
  - **Fuite d'informations**
    - **http://developer.joomla.org/security/news/9-security/10-core-security/340-20110401-core-information-disclosure.html**

- **Joomla! < 1.6.1**
  - **http://developer.joomla.org/security/news/328-20110201-core-sql-injection-path-disclosure**
  - **http://developer.joomla.org/security/news/329-20110202-core-path-disclosure**
  - **http://developer.joomla.org/security/news/330-20110203-core-xss-vulnerabilities**
  - **http://developer.joomla.org/security/news/331-20110204-core-xss-vulnerabilities**
  - **http://developer.joomla.org/security/news/332-20110301-core-information-disclosure**
  - **http://developer.joomla.org/security/news/333-20110302-core-redirect-vulnerabilities**
  - **http://developer.joomla.org/security/news/334-20110303-core-information-disclosure**
  - **http://developer.joomla.org/security/news/335-20110304-core-unauthorised-access**
  - **http://developer.joomla.org/security/news/336-20110305-core-csrf-vulnerability**
  - **http://developer.joomla.org/security/news/337-20110306-core-dos-vulnerabilities**
  - **http://developer.joomla.org/security/news/338-20110307-core-xss-vulnerabilities**
  - **http://developer.joomla.org/security/news/339-20110308-core-csrf-vulnerability**

Infos Unix

- Moodle
  - http://moodle.org/mod/forum/discuss.php?d=170002
  - http://moodle.org/mod/forum/discuss.php?d=170003
  - http://moodle.org/mod/forum/discuss.php?d=170004
  - http://moodle.org/mod/forum/discuss.php?d=170005
  - http://moodle.org/mod/forum/discuss.php?d=170006
  - http://moodle.org/mod/forum/discuss.php?d=170008
  - http://moodle.org/mod/forum/discuss.php?d=170009
  - http://moodle.org/mod/forum/discuss.php?d=170010
  - http://moodle.org/mod/forum/discuss.php?d=170011
  - http://moodle.org/mod/forum/discuss.php?d=170012

Infos Unix

- Majordomo < 20110204
  - Le correctif précédent était insuffisant
    - https://bugzilla.mozilla.org/show_bug.cgi?id=631307
- Mailman < 2.1.14
  - XSS
    - http://www.debian.org/security/2011/dsa-2170
- LogWatch
  - Exécution de commandes via un nom de fichier
    - http://sourceforge.net/tracker/?func=detail&aid=3184223&group_id=312875&atid=1316824
- LogRotate … aussi
  - Ou presque
    - http://rhn.redhat.com/errata/RHSA-2011-0407.html
- Subversion
  - Déni de service (?)
    - http://subversion.apache.org/security/CVE-2011-0715-advisory.txt

Infos Unix

- Apache ActiveMQ
  - Directory Traversal
    - http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=895
- Citrix XenApp
  - Exécution de code à distance (via XML-RPC)
    - http://support.citrix.com/article/CTX128169
- Citrix Secure Gateway 3.1.4
  - Exécution de code à distance
    - http://support.citrix.com/article/CTX128168
- OpenLDAP < 2.4.24
    - http://www.openldap.org/its/index.cgi/Software%20Bugs?id=6661
    - http://www.openldap.org/its/index.cgi/Software%20Bugs?id=6607
- Mac OS X ftpd
  - Enumération du tout le disque (0day)
    - http://archives.neohapsis.com/archives/fulldisclosure/2011-02/0269.html

Infos Unix

- ClamAV
  - Exécution de code (?)
    - https://wwws.clamav.net/bugzilla/show_bug.cgi?id=2486
- chfn et chsh permettent d'altérer le fichier /etc/passwd
    - https://lwn.net/Articles/428248/
- AIX 6.1
  - Il est possible de s'authentifier en LDAP avec un mauvais mot de passe
    - http://aix.software.ibm.com/aix/efixes/security/ldapauth_advisory.asc
- FreeBSD: fuite d'information via crontab
    - http://archives.neohapsis.com/archives/fulldisclosure/2011-02/0660.html
- F-Secure Internet Gateway pour Linux
  - Accès aux fichiers de log sans authentification
    - http://www.f-secure.com/en_EMEA/support/security-advisory/fsc-2011-1.html

Infos Unix

- Autre
  - PHP.NET compromis
    - Les sources de PHP ont été "backdoorées"
    - Et ça n'est pas la première fois
      - http://bjori.blogspot.com/2010/12/php-project-and-code-review.html
  - Fin de support pour FreeBSD 7.1
  - Sortie de Debian 6 (Squeeze)
    - Le support IPv6 est intégré au noyau par défaut
  - Debian se met "sérieusement" à la sécurité (ou pas)
    - http://lpsolit.wordpress.com/2011/03/04/debian-takes-security-very-seriously-but-how/
  - Sortie de MySQL 5.5 en version "entreprise"
  - On parie ?
    - http://buzz.typo3.org/teams/security/article/typo3-45-will-be-the-most-secure-typo3-version-ever/

Failles

- **Principales applications**
  - **Adobe ShockWave < 11.5.9.620**
    - **21 failles corrigées par APSB11-01**
      - **http://www.adobe.com/support/security/bulletins/apsb11-01.html**
      - **ZDI-11-078 … ZDI-11-081**
    - **Crédits**
      - **Carsten Eiram / Secunia Research (x3)**
      - **Krystian Kloskowski (h07) / Secunia Research**
      - **Aniway & Luigi Auriemma / ZDI**
      - **Aniway / ZDI**
      - **Luigi Auriemma / ZDI**
      - **anonymous / ZDI**
      - **anonymous / ZDI**
      - **Logan Brown & Aaron Portnoy / TippingPoint DVLabs**
      - **Aaron Portnoy & Logan Brown / TippingPoint DVLabs (x4)**
        - **TPTI-11-01 … TPTI-11-05**
      - **Mark Yason / IBM's X-Force (x2)**
      - **Will Dormann / CERT/CC (x5)**
      - **Andrzej Dyjak / iDefense Labs**

Failles

- Adobe Flash Player < 10.2.152.26
  - 13 failles corrigées par APSB11-02
    - http://www.adobe.com/support/security/bulletins/apsb11-02.html
  - Crédits
    - anonymous / ZDI
    - Vitaliy Toropov / iDefense VCP
      - http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=893
    - Anonymous / iDefense VCP
      - http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=894
    - Tavis Ormandy / Google (x2)
    - Bo Qu / Palo Alto Networks (x4)
    - Will Dormann / CERT (x2)
    - Simon Raner / ACROS Security
    - Marc Schoenefeld / Red Hat Security Response Team

- Adobe Flash Player < 10.2.153.1
  - Corrige une faille exploitée en "0day" dans de nombreuses attaques ciblées
    - http://www.adobe.com/support/security/bulletins/apsb11-05.html
  - Cette fois c'st sûr, ce sont les chinois … ou pas ☺
    - http://blog.fireeye.com/research/2011/03/who-is-exploiting-the-flash-0-day-cve-2011-0609.html

Failles

- Adobe Reader < 9.4.2, < 10.0.1
  - 29 failles corrigées par APSB11-03
    - http://www.adobe.com/support/security/bulletins/apsb11-03.html
  - ZDI-11-065 … ZDI-11-075 + ZDI-11-077
  - Crédits
    - Tavis Ormandy / Google (x3)
    - Billy Rios / Google (x2)
    - Bing Liu / Fortinet's FortiGuard Labs
    - Haifei Li / Fortinet's FortiGuard Labs
    - Peter Vreugdenhil / ZDI (x7)
    - Sebastian Apelt / ZDI
    - el / ZDI
    - Abdullah Ada / ZDI
    - anonymous / ZDI
    - (…)

Failles

- Mitja Kolsek / ACROS Security
- James Quirk / Los Alamos
- Brett Gervasoni / Sense of Security
- Joe Schatz / United States Senate, Office of the Sergeant at Arms, IT Security
- Greg MacManus / iSIGHT Partners Labs
- Sean Larsson / iDefense Labs
  - http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=891
- Will Dormann / CERT
- Marc Schoenefeld / Red Hat Security Response Team
- CESG
- Matthew Pun
- Parvez Anwar

- **Adobe Reader < 9.4.3, < 10.0.2**
  - **Corrige une faille exploitée en "0day" dans de nombreuses attaques ciblées**
    - **http://www.adobe.com/support/security/bulletins/apsb11-06.html**

Failles

- Adobe ColdFusion
  - 5 failles corrigées par APSB11-004
    - XSS, CRLF injection, fuite d'information, Session Fixation
      - http://www.adobe.com/support/security/bulletins/apsb11-04.html
    - Exploitation triviale
      - http://www.doecirc.energy.gov/bulletins/t-549.shtml
  - Crédits
    - Richard Brain / ProCheckUp Ltd
    - HongZhen Zhou / McAfee
    - Tenable Network Security
    - Bogdan Calin
    - Michael Dominice
    - Pete Freitag / Foundeo
    - Tom Sellers / FadedCode
    - Chad Armond
    - Jason Dean / 12robots

Failles

- Oracle Java
  - Java < 1.6.0_24, < 1.5.0_27, < 1.4.2_30
    - Entre 20 et 25 failles corrigées (dont des failles d'exécution de code)
      - http://www.oracle.com/technetwork/topics/security/javacpufeb2011-304611.html
      - ZDI-11-082 … ZDI-11-086
      - http://slightlyrandombrokenthoughts.blogspot.com/2011/02/java-jfilechooser-programmatic.html
      - http://slightlyrandombrokenthoughts.blogspot.com/2011/03/oracle-java-applet-clipboard-injection.html
    - La faille "*floating point*" a été corrigée par ailleurs
      - http://www.oracle.com/technetwork/topics/security/alert-cve-2010-4476-305811.html
- Google Chrome < 10.0.648.204
- FireFox < 3.6.16
  - Bloque les certificats Comodo frauduleux
- ThunderBird < 3.1.8
    - http://www.mozilla.org/security/known-vulnerabilities/thunderbird31.html#thunderbird3.1.8
  - Immédiatement suivie par ThunderBird 3.1.9

Failles

- Safari < 5.0.4
  - http://support.apple.com/kb/HT4566
- Apple iTunes < 10.2
  - http://support.apple.com/kb/HT4554
  - http://lists.apple.com/archives/security-announce/2011/Mar/msg00000.html
- Apple iOS 4.3
  - 49 failles … rien que dans Safari
    - http://support.apple.com/kb/HT4564
- Apple Mac OS X < 10.6.7
  - http://support.apple.com/kb/HT4581
- Mise à jour Java pour Mac OS X 10.5 et 10.6
  - http://support.apple.com/kb/HT4562
  - http://support.apple.com/kb/HT4563
- Note: avec Mac OS X 10.7 "Lion"
  - … Apple découvre les vertus de l'audit de sécurité "gratuit"
    - http://www.edibleapple.com/apple-asks-security-experts-to-examine-os-x-lion/
    - http://www.pcworld.com/article/221368/apple_gets_quietly_serious_about_security.html

Failles

- **WireShark < 1.4.4**
  - **http://www.wireshark.org/security/wnpa-sec-2011-03.html**
  - **http://www.wireshark.org/security/wnpa-sec-2011-04.html**
- **RealPlayer < 14.0.2, RealPlayer Enterprise < 2.1.5**
  - **ZDI-11-076**
- **VLC < 1.1.7**
  - **http://www.videolan.org/security/sa1102.html**
- **Foxit Reader < 4.3.1.0218**
  - **Faille triviale d'accès aux fichiers**
    - **http://scarybeastsecurity.blogspot.com/2011/03/dangerous-file-write-bug-in-foxit-pdf.html**
- **muPDF <= 0.7**
  - ***Integer overflow* (x2) remontés par Secunia**
    - **http://secunia.com/secunia_research/2011-12/**
- **SumatraPDF < 1.3**
  - ***Integer overflow* (x2) remontés par Secunia (les mêmes !)**
    - **http://secunia.com/secunia_research/2011-13**

Failles

- CA HIPS
  - Exécution de code au travers du contrôle ActiveX
    - https://support.ca.com/irj/portal/anonymous/phpsupcontent?contentID={53A608DF-BFDB-4AB3-A98F-E4BB6BC7A2F4}
- Lotus Notes 8
  - Failles multiples
    - ZDI-11-045 … ZDI-11-053 (sauf ZDI-10-050 qui concerne Informix)
    - http://www-01.ibm.com/support/docview.wss?uid=swg21461514
  - Note: publiées par ZDI après l'expiration du délai de 180 jours
- Cisco Security Agent Management Center
  - ZDI-11-088: création de fichiers arbitraires sans authentification
    - http://www.cisco.com/warp/public/707/cisco-sa-20110216-csa.shtml
- VMWare ESX
  - Déni de service sur Cisco Nexus 1000V
    - http://www.vmware.com/security/advisories/VMSA-2011-0002.html
  - Et aussi …
    - http://www.vmware.com/security/advisories/VMSA-2011-0003.html
    - http://www.vmware.com/security/advisories/VMSA-2011-0004.html
- VMWare WorkStation < 7.1.4
    - http://www.vmware.com/security/advisories/VMSA-2011-0006.html

Failles

- Xerox WorkCenter
  - Faille Samba potentiellement exploitable
    - http://www.xerox.com/downloads/usa/en/c/cert_XRX11-002_v1.0.pdf
  - Exécution de commandes via l'interface Web
    - http://www.xerox.com/downloads/usa/en/c/cert_XRX11-001_v1.0.pdf
- Sun One ?
    - http://twitpic.com/44zahd

- Une faille Adobe Reader …
  - $5 million au marché noir (?!?)
    - http://www.infosecurity-magazine.com/view/15889/interview-matt-moynahan-ceo-veracode/

Failles 2.0

- Les sites piratés du mois (1/2)
  - Bercy
  - Commission Européenne & Parlement Européen
  - Comodo
    - Plusieurs certificats frauduleux émis
      - https://www.comodo.com/Comodo-Fraud-Incident-2011-03-23.html
    - Révoqués "en dur" dans les principaux navigateurs
    - Espérons que cette explication soit fausse …
      - http://pastebin.com/74KXCaEZ
      - http://pastebin.com/DBDqm6Km
  - RSA
    - Tous les clients de la solution SecurID pourraient être affectés par le vol des "graines" secrètes
      - http://blogs.rsa.com/rivner/anatomy-of-an-attack/
    - Comment lire ses logs SecurID
      - http://isc.sans.edu/diary.html?storyid=10618
    - Remarque: il y a des failles dans le produit par ailleurs
      - http://www.securityfocus.com/archive/1/archive/1/517023/100/0/threaded

Failles 2.0

- Les sites piratés du mois (2/2)
  - PHP
    - Wiki + code source (?)
      - http://blog.phpfog.com/2011/03/22/how-we-got-owned-by-a-few-teenagers-and-why-it-will-never-happen-again/
  - La liste "vendor-sec"
    - http://permalink.gmane.org/gmane.comp.security.oss.general/4350
  - MySQL
    - Via une injection SQL …
      - http://tinkode27.baywords.com/mysql-com-fr-it-de-jp-full-disclosure-hacked-by-tinkode-and-ne0h/
  - London Stock Exchange
    - http://www.highseverity.com/2011/02/london-stock-exchange-hit-by-malware.html
  - TripAvisor
    - 40,000,000 comptes

Failles 2.0

- Epsilon
  - L'une des plus grosses plateformes d'*emailing* américaine
    - http://yro.slashdot.org/story/11/04/04/160214/Epsilon-Breach-Affects-JPMorgan-Chase-Capital-One
- Forums WinAmp
    - http://forums.winamp.com/showthread.php?t=327374
- ECCouncilAcademy.org
    - http://s2.kimag.es/share/90829065.png
- Fédération UMP de la Vienne
  - Fuite de données accidentelle … depuis 8 mois
    - http://www.zataz.com/news/21054/fuite--donnees--nominatives--ump.html
- Et probablement plein d'autres …
  - Samsung TV (?)
    - http://pastebin.com/rD8hwpxT

Failles 2.0

- Les sociétés pétrolières victimes d'intrusions ciblées
  - Opération "Night Dragon"
    - http://blogs.mcafee.com/corporate/cto/global-energy-industry-hit-in-night-dragon-attacks
- NASDAQ
  - La NSA officiellement sollicitée
- Ce que révèlent les emails de HBGary …
  - De nombreuses intrusions ne sont pas reportées, même en cas d'obligation légale
    - https://www.infosecisland.com/blogview/12420-HBGary-Federal-Emails-Reveal-More-Unreported-Attacks.html

Failles 2.0

- LizaMoon
  - Un nouvelle vague d'injections SQL en masse
  - Plus d'un million de sites compromis (?)
- 35 failles SCADA d'un coup
  - http://seclists.org/bugtraq/2011/Mar/187
- Twitter FAIL (again!)
  - http://bostinnovation.com/2011/02/03/how-i-discovered-a-security-vulnerability-in-twitter-that-impacted-1-5-million-users/
- Anonymous déclare la guerre à Koch Industries
  - http://anonnews.org/?p=press&a=item&i=585

Failles 2.0

- **Une faille de sécurité**
  - **Dans un exemple de code publié par Mastercard**
    - **http://jack-mannino.blogspot.com/2011/02/scary-scary-mobile-banking.html**
- **Les députés du Missouri victimes de FireSheep**
    - **http://nakedsecurity.sophos.com/2011/02/08/free-open-wifi-facebook-hack-missouri-state-representatives/**

Malwares et spam

- ZeuS sur Symbian et Windows Mobile
  - Pour capturer les mTANs
    - http://www.f-secure.com/weblog/archives/00002104.html
- Microsoft et FireEye mettent fin au botnet Rustock
    - http://blogs.technet.com/b/mmpc/archive/2011/03/18/operation-b107-rustock-botnet-takedown.aspx
- McAfee rachète Sentrigo
    - http://www.mcafee.com/us/about/mcafee-sentrigo.aspx
- Samsung: ce ne sont pas les *keyloggers* que vous cherchez
    - http://www.f-secure.com/weblog/archives/00002133.html
  - CISSP MSIA CISA #fail
    - http://www.networkworld.com/newsletters/sec/2011/032811sec2.html
- Le meilleur moyen d'infecter une application Android ?
  - Payer son développeur pour le faire !
    - http://www.reddit.com/r/Android/comments/fm3cu/spyware_company_wants_us_to_embed_their_code_into/

Malwares et spam

- Un général israélien se vante d'être l'auteur de StuxNet
  - … lors de son pot de départ
    - http://www.richardsilverstein.com/tikun_olam/2011/02/14/ashkenazi-video-claims-idf-responsibility-for-bombing-syrian-nuclear-reactor-and-stuxnet/
    - http://www.net-security.org/secworld.php?id=10596
- Le 8 février, c'était le Safer Internet Day
    - http://www.saferinternet.org/web/guest/safer-internet-day

Actualité (francophone)

- Le ministère du budget "piraté"
- La "vrai fausse" affaire du ministère des affaires étrangères
  - http://sid.rstack.org/blog/index.php/463-apres-bercy-le-quai-d-orsay
  - http://sid.rstack.org/blog/index.php/464-le-vrai-fail-du-quai-d-orsay
- Une DSI inter-ministérielle pour l'état
  - La DISIC
- Le décret sur la conservation des données de publication en ligne fait débat
  - http://www.legifrance.gouv.fr/affichTexte.do;jsessionid=?cidTexte=JORFTEXT000023646013&dateTexte=&oldAction=rechJO&categorieLien=id
- La DCRI casse les codes de l'ETA
  - … ou pas
    - http://www.intelligenceonline.fr/renseignement-d-etat/les-organisations/2011/02/17/la-dcri-a-casse-les-codes-de-l-eta,88096860-ART

Actualité (francophone)

- La stratégie de cyber sécurité de la France
  - L'ANSSI pilote la "cyber défense" en cas de "cyber guerre"
    - http://www.ssi.gouv.fr/site_article318.html
- Skype illégal en France ?
  - Faute d'interception légale
    - http://blogs.lexpress.fr/tic-et-net/2011/02/22/le-service-skype-illegal-en-france/
- Partenariat EPITA / OCLCTIC
    - http://www.globalsecuritymag.fr/L-OCLCTIC-et-l-EPITA-signent-une,20110215,22056.html
- Enquête de l'INSEE sur les TIC
    - http://www.insee.fr/fr/themes/document.asp?ref_id=tic10
- La femme de ménage fait débat
    - http://bugbrother.blog.lemonde.fr/2011/01/06/larmee-privatise-le-nettoyage-de-ses-grandes-oreilles/
- Des clés USB cachées dans Paris
    - http://blog.culturemobile.net/index.php/2010/12/15/538-cles-usb-paris-ville-art-p2p-fichiers-dead-drops

Actualité (anglo-saxonne)

- L'USAF lance un appel d'offres
  - Pour créer massivement de faux profils sur les réseaux sociaux
    - http://www.federalnewsradio.com/?nid=15&sid=2282156
- Cyber 3.0: cette fois, c'est la guerre
    - http://www.securityvibes.com/community/fr/blog/2011/02/16/les-etats-unis-font-officiellement-du-cyber-un-nouveau-champ-de-bataille
- Autres nouvelles législatives
    - http://www.govinfosecurity.com/articles.php?art_id=3367
- Le gouvernement américain escroqué
  - … par un soi-disant vendeur de "cyber-défense"
    - http://www.nytimes.com/2011/02/20/us/politics/20data.html
- Le Canada piraté
    - http://www.cbc.ca/politics/story/2011/02/16/pol-weston-hacking.html

Actualité (européenne)

- Des négociations secrètes sur le droit d'auteur
  - http://hightech.nouvelobs.com/actualites/depeche/20110131.OBS7251/telechargement-les-negociations-secretes-de-bruxelles.html

Actualité (Google)

- L'authentification 2 facteurs pour tous !
  - http://googleblog.blogspot.com/2011/02/advanced-sign-in-security-for-your.html
- Gmail perd 150,000 comptes
  - http://news.cnet.com/8301-1023_3-20037019-93.html
- La fin de la barre d'URL ?
  - http://www.conceivablytech.com/5746/products/google-may-kill-chrome-url-bar
- Quelques condamnations en France
  - CNIL (Google Street View)
    - http://www.cnil.fr/la-cnil/actu-cnil/article/article/google-street-view-la-cnil-prononce-une-amende-de-100-000-euros/
  - Contrefaçon (Google Vidéo)
    - http://www.pcinpact.com/actu/news/62364-google-image-filtrage-contrefacon-notice-and-stay-down.htm
  - Droit à l'oubli
    - http://www.pcinpact.com/actu/news/62496-cnil-institutrice-desindexation-google-moteur.htm

Actualité (Google)

- Google vs. Chine, ça n'est pas fini
  - http://www.zdnet.fr/actualites/gmail-la-chine-rejette-les-accusations-de-censure-de-google-39759275.htm
  - http://www.zdnet.fr/actualites/la-chine-sanctionne-trois-entreprises-liees-a-google-pour-fraude-fiscale-39759590.htm
- Google vs. Reste du monde
  - http://www.clubic.com/connexion-internet/actualite-402262-turquie-bloque-blogger.html
- Recrutements, acquisitions, partenariats
  - James Gosling (ex-patron de Java chez Oracle)
  - Zynamics
    - http://blog.zynamics.com/2011/03/01/zynamics-acquired-by-google/
  - Dasient, Inc.
    - Lutte contre les publicités malveillantes
    - Fondée par des anciens de Google
      - http://www.techtree.com/India/News/Google_Invests_in_Anti-malware_Start-up/551-114416-582.html
  - CNRS
    - http://www2.cnrs.fr/presse/communique/2093.htm

Actualité (crypto)

- Le *keychain* de l'iPhone ne tient pas 6 minutes
  - http://www.infoworld.com/d/mobilize/iphone-attack-reveals-passwords-in-six-minutes-050
- De la stégano vraiment utile
  - MP4 + TrueCrypt
    - http://lifehacker.com/#!5771142/embed-a-truecrypt-volume-in-a-playable-video-file
- Partenariat Xilinx / ARM
  - http://www.fpgagurus.edn.com/blog/fpga-gurus-blog/xilinx-christens-zynq-7000-family-embedded-arm

Actualité

- Sorties logicielles
  - FireFox 4.0
    - https://developer.mozilla.org/en/Firefox_4_for_developers#Security
  - Metasploit 3.5.2
    - Corrige une faille de sécurité !
      - http://blog.metasploit.com/2011/02/metasploit-framework-352-released.html
  - Metasploit 3.6.0
    - Ajoute le support SAP
      - http://blog.metasploit.com/2011/03/metasploit-framework-360-released.html
  - Python 3.2
  - BugCheck: un SoftIce Open Source
    - http://bugchecker.com/
  - $3000 pour une faille de sécurité dans Hex-Rays
    - http://www.hex-rays.com/bugbounty.shtml
  - Concours de plugins Hex-Rays jusqu'au 15 juillet
    - http://www.hex-rays.com/contest.shtml

Actualité

- Conférences à venir
  - Hackito Ergo Sum
    - 7-9 avril à Paris
      - http://hackitoergosum.org/
  - Solutions Linux
    - 10-12 mai à La Défense
      - http://www.solutionslinux.fr/
  - SSTIC
    - 8-10 juin à Rennes
      - http://www.sstic.org/2011/programme/
  - Hack In Paris
    - 14-17 juin à Disneyland
      - http://www.hackinparis.com/
  - ReCON
    - 8-10 juillet à Montréal
      - http://www.recon.cx/

Actualité

- Conférences passées
  - CanSecWest 2011
    - Et le désormais célèbre "pwn2own"
      - Sont tombés: Safari / Mac OS X, IE8, terminal BlackBerry
      - A résisté: Chrome
      - http://blog.internetnews.com/skerner/2011/03/why-pwn2own-doesnt-target-linu.html
    - Félicitations à VUPEN ☺
    - Un challenge de plus en plus contesté …
      - http://www.computerworld.com/s/article/9211720/Three_time_Pwn2Own_winner_knocks_hacking_contest_rules
- Quelques initiatives de standardisation
  - Continuité d'activité
    - ISO 22301
  - IASME - Information Assurance for SMEs
    - http://www.ncc.co.uk/article/?articleid=16315

Actualité

- Pour les *pentesteurs*
  - http://pentest-standard.org/
  - http://code.google.com/p/pentest-bookmarks
  - http://pwnieexpress.com/

Actualité

- Un brevet Cenzic redoutable
  - Couvre toute forme de XSS ou d'injection SQL
    - http://www.stop232patent.com/
- Le nouveau port "ThunderBolt" fait débat
    - http://erratasec.blogspot.com/2011/02/thunderbolt-introducing-new-way-to-hack.html
- La Chine panique
  - Désormais le simple fait de prononcer le mot "*protest*" au téléphone coupe la communication
    - http://www.nytimes.com/2011/03/22/world/asia/22china.html
- Après WikiLeaks
  - Après OpenLeaks
    - http://anonleaks.ru/
- Julian Assange va être extradé vers la Suède

Fun

- ***Never Say Hello***
  - http://seclists.org/fulldisclosure/2011/Mar/342
  - 3 jours après
    - http://seclists.org/fulldisclosure/2011/Mar/418
- **Une bonne application Android**
  - Elle ouvre des portes ☺
    - http://www.cybersecurityguy.com/caribou.html
- **Ils l'ont fait**
  - http://www.lexpress.fr/actualite/monde/le-bebe-facebook-est-nee-en-egypte_964620.html

Questions / réponses

- Questions / réponses
- Prochaine réunion
  - Mardi 17 mai 2011
- N'hésitez pas à proposer des sujets et des salles