OSSIR
Groupe Paris

Réunion du 9 novembre 2010

Revue des dernières vulnérabilités

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

Avis Microsoft

- **Octobre 2010**
  - **16 bulletins, 49 failles**
  - **Références**
    - **http://www.microsoft.com/technet/security/bulletin/ms10-oct.mspx**
    - **http://blogs.technet.com/b/msrc/archive/2010/10/11/october-2010-security-bulletin-release.aspx**
    - **http://blogs.technet.com/b/msrc/archive/2010/10/18/q-amp-a-from-the-october-2010-security-bulletin-webcast.aspx**
    - **http://blogs.technet.com/b/srd/archive/2010/10/12/note-on-bulletin-severity-for-ms10-081-and-ms10-074.aspx**
    - **http://blogs.technet.com/b/srd/archive/2010/10/12/assessing-the-risk-of-the-october-security-updates.aspx**
  - **MS10-071 Correctif cumulatif pour Internet Explorer [?,3,3,3,1,?,1,3,1]**
    - **Affecte: Internet Explorer (toutes versions supportées)**
    - **Exploit: fuite d'information, exécution de code, …**
      - **http://www.80vul.com/ie8/IE8%20Css%20Cross-Domain%20Information%20Disclosure%20Vulnerability.txt**
      - **http://archives.neohapsis.com/archives/fulldisclosure/2010-10/0143.html**
      - **http://www.coresecurity.com/content/MS-Office-HtmlDlgHelper-memory-corruption**
      - **http://www.zerodayinitiative.com/advisories/ZDI-10-197/**
      - **http://scarybeastsecurity.blogspot.com/2010/10/minor-leak-major-headache.html**

Avis Microsoft

  - Crédit:
    - Sirdarckcat / Google
    - Mario Heiderich
    - Takehiro Takahashi / IBM ISS X-Force
    - Peter Vreugdenhil / ZDI
    - Damián Frizza / Core
    - Aldwin Saugere & Radoslav Vasilev / Cigital
    - Rodrigo Rubira Branco / Check Point IPS Research Center

- MS10-072 Failles dans SafeHTML [3,3]
  - Affecte:
    - SharePoint Services 3.0
    - SharePoint Foundation 2010
    - SharePoint Server 2007
    - Groove Server 2010
    - Office Web Apps
  - Exploit: mauvais filtrage du HTML créé par l'utilisateur, pouvant conduire à des XSS
    - http://archives.neohapsis.com/archives/fulldisclosure/2010-08/0179.html
  - Crédit:
    - Sirdarckcat / Google
    - Mario Heiderich

Avis Microsoft

- MS10-073 Failles noyau [3,1,1]
  - Affecte: Windows (toutes versions supportées)
    - Plus exactement WIN32K.SYS
  - Exploit: élévations de privilèges locales
    - Dont la faille "layout clavier" exploitée par StuxNet
      - http://blog.eset.com/2010/10/15/win32k-sys-about-the-patched-stuxnet-exploit
  - Crédit:
    - Sergey Golovanov, Alexander Gostev, Maxim Golovkin, Alexey Monastyrsky / Kaspersky Lab
    - Vitaly Kiktenko & Alexander Saprykin / Design and Test Lab
    - Eric Chien / Symantec
    - Tarjei Mandt / Norman

Avis Microsoft

- **MS10-074 Faille dans la MFC [?]**
  - **Affecte: Windows (toutes versions supportées)**
  - **Exploit: *buffer overflow* lors de la mise à jour du titre d'une fenêtre**
    - **Une faille publiée depuis longtemps !**
    - **Initialement détectée dans PowerZip**
      - **http://secunia.com/advisories/40298/**
  - **Crédit: Carsten H. Eiram / Secunia**

- **MS10-075 Faille dans Media Player Network Sharing Service [1]**
  - **Affecte: Windows Vista, Windows Seven**
  - **Exploit: *use-after-free* dans le support du protocole RTSP**
    - **http://www.zerodayinitiative.com/advisories/ZDI-10-199/**
  - **Crédit: Oleksandr Mirosh / ZDI**

Avis Microsoft

- MS10-076 Faille dans le support des polices OpenType [1]
  - Affecte: Windows (toutes versions supportées)
  - Exploit: *integer overflow*
    - http://www.zerodayinitiative.com/advisories/ZDI-10-198/
    - http://siberas.de/advisories/advisories_2010.html
  - Crédit:
    - Sebastian Apelt / ZDI
    - Ivan Fratric / iSIGHT Partners Global Vulnerability Partnership

- MS10-077 Faille dans le .NET Framework [1]
  - Affecte: .NET Framework 4.0
    - Sur plateformes 64 bits uniquement
  - Exploit: évasion de la machine virtuelle
    - http://connect.microsoft.com/VisualStudio/feedback/details/578948/x64-jit-stack-overflow#
    - http://weblog.ikvm.net/PermaLink.aspx?guid=d2f792af-a629-4056-ae86-d7deeaa16a1c
  - Crédit: Jeroen Frijters / Sumatra

Avis Microsoft

- **MS10-078 Failles dans le support des polices OpenType [1,1]**
  - **Affecte: Windows XP / 2003**
  - **Exploit: élévations de privilèges locales**
    - **http://www.coresecurity.com/content/ms-opentype-cff-parsing-vulnerability**
    - **http://siberas.de/advisories/advisories_2010.html**
  - **Crédit:**
    - **Sebastian Apelt / siberas**
    - **Diego Juarez / Core**

- **MS10-079 Failles dans Word [1,1]**
  - **Affecte: Word (toutes versions supportées, y compris Mac OS, Viewer, packs de compatibilité et Office Web Apps)**
    - **Non affecté: Works 9**
  - **Exploit: *overflows* divers**
  - **Crédit:**
    - **Nicolas Joly / VUPEN**
    - **Chaouki Bekrar / VUPEN (x10)**

Avis Microsoft

- MS10-080 Failles dans Excel [1,1,1,1,1,1]
  - Affecte: Excel (toutes versions supportées, sauf 2010)
    - Non affecté: Works 9
  - Exploit: *overflows* divers
    - http://secunia.com/secunia_research/2010-55/
    - http://secunia.com/secunia_research/2010-63/
    - http://secunia.com/secunia_research/2010-64/
    - http://secunia.com/secunia_research/2010-65/
  - Crédit:
    - Chaouki Bekrar / VUPEN (x10)
    - Carsten H. Eiram / Secunia (x2)
    - Alin Rad Pop / Secunia (x2)
    - Omair

- MS10-081 Faille dans COMCTL32.DLL [1]
  - Affecte: Windows (toutes versions supportées)
  - Exploit: *heap overflow* dans le support SVG
    - Cette interface n'est pas utilisée par les applications Microsoft
  - Crédit: Krystian Kloskowski (h07) / Secunia

Avis Microsoft

- MS10-082 Faille dans Windows Media Player [1]
  - Affecte: Windows Media Player 9 / 10 / 11 / 12
  - Exploit: mauvaise réallocation d'objet par le lecteur
    - http://skypher.com/index.php/2010/10/12/issue-21-wmp-memory-corruption-using-popups/
    - http://code.google.com/p/skylined/issues/detail?id=21
    - A priori non exploitable depuis Internet Explorer ?
  - Crédit: SkyLined / Google

- MS10-083 Faille dans le support des objets COM [1]
  - Affecte: Windows Shell, WordPad
  - Exploit: mauvaise gestion des composants COM lors de l'accès à un partage réseau (Windows Shell) ou de l'ouverture d'un fichier (WordPad)
  - Crédit:
    - HD Moore / Rapid7
    - David Dewey / IBM ISS X-Force
    - Ryan Smith / Accuvant

Avis Microsoft

- **MS10-084 Faille dans le support des LPC [1]**
  - **Affecte: Windows XP / 2003**
  - **Exploit: élévation de privilèges locale**
    - ***Buffer overflow* dans RPCSS.EXE**
    - **http://seclists.org/fulldisclosure/2010/Oct/84**
  - **Crédit: n/d**

- **MS10-085 Faille dans SChannel [3]**
  - **Affecte: Windows Vista / 2008 / Seven / 2008R2**
  - **Exploit: déni de service sur TLSv1**
    - **Crash de LSASS.EXE**
  - **Crédit: Mu Dynamics**

Avis Microsoft

- MS10-086 Faille dans Microsoft Cluster Service (MSCS) [?]
  - Affecte: Windows 2008 R2
  - Exploit: les permissions par défaut attachées à un cluster de disques sont incorrectes
    - "Tout le monde: Contrôle Total" sur le partage administratif ☺
    - http://blogs.technet.com/b/srd/archive/2010/10/12/ms10-086-disk-clustering-vulnerability.aspx
  - Crédit: n/d

Avis Microsoft

- **Prévisions Microsoft pour novembre**
  - **3 bulletins, 11 failles**
    - **Office**
    - **PowerPoint**
    - **ForeFront**

Avis Microsoft

- Advisories
  - Q2458511 Faille Internet Explorer (toutes versions supportées)
    - V1.0: publication de l'*advisory*
    - V1.1: mesures de contournement
      - http://blogs.technet.com/b/srd/archive/2010/11/03/dep-emet-protect-against-attacks-on-the-latest-internet-explorer-vulnerability.aspx
    - Détecté "dans la nature" … et déjà disponible dans Metasploit
      - http://extraexploit.blogspot.com/2010/11/cve-2010-3962-yet-another-internet.html
  - Q2416728 Faille ASP.NET
    - V2.0: correctif publié
  - Q973811 "Extended Protection for Authentication"
    - V1.7: ajout du protocole SMB

Avis Microsoft

- Révisions
  - MS10-077
    - V1.2: changement de la logique de détection

Infos Microsoft

- Sorties logicielles
  - Windows Seven SP1 (RC1)
  - Exchange 2010 SP1
  - Office 365
  - System Center Configuration Manager 2007 R3
  - Microsoft Security Intelligence Report (SIR), volume 9
    - http://www.microsoft.com/security/sir/default.aspx
    - La JVM devient la cible privilégiée des malwares
      - http://blogs.technet.com/b/mmpc/archive/2010/10/18/have-you-checked-the-java.aspx
  - Un portail regroupant tous les outils de sécurité Microsoft
    - http://technet.microsoft.com/en-us/security/cc297183.aspx

Infos Microsoft

- **Autre**
  - **Microsoft s'associe à Cloud.com / OpenStack**
    - http://cloud.com/company/blog/microsoft-and-cloud-partner-to-bring-hyper-v-to-openstack
    - http://openstack.org/
  - **Windows Live Spaces passe sous WordPress**
    - http://en.blog.wordpress.com/2010/09/27/welcome-windows-live-spaces-bloggers/
  - **Microsoft pourrait racheter Adobe**
    - http://bits.blogs.nytimes.com/2010/10/07/microsoft-and-adobe-chiefs-meet-to-discuss-partnerships/
  - **… ou pas**
    - **Microsoft et Adobe veulent surtout faire barrage à Apple sur le marché de la téléphonie mobile**
      - http://www.solutions-logiciels.com/actualites.php?actu=8368
    - **Apple, futur MVNO ?**
      - http://www.linformaticien.com/Actualit%C3%A9s/tabid/58/newsid496/9380/apple-associe-avec-gemalto-souhaite-devenir-mvno/Default.aspx
  - **Ray Ozzie part à la retraite**
    - **Responsable des projets SilverLight, Azure, … (entre autres)**

Infos Réseau

- (Principales) faille(s)
  - Crash dans ISC DHCP 4.x
    - Grâce à IPv6 …
      - http://www.isc.org/software/dhcp/advisories/cve-2010-3611
  - Faille exploitable à distance sans authentification dans CiscoWorks
    - Buffer overflow(s)
      - http://www.cisco.com/warp/public/707/cisco-sa-20101027-cs.shtml
  - Failles multiples dans Cisco ICM Setup Manager Agent.exe
    - ZDI-10-232, ZDI-10-233, ZDI-10-234, ZDI-10-235
  - Binaire "setuid" vulnérable dans Cisco Unified Communications Manager
      - http://tools.cisco.com/security/center/viewAlert.x?alertId=21656

Infos Réseau

- **Autres infos**
  - **DNSSEC poursuit son chemin**
    - **Signature effective du ".com" et du ".net" le 9 décembre**
      - **http://isc.sans.edu/diary.html?storyid=9883**
  - **Tous les CheckPoint UTM-1 ont rebooté le 30 octobre à minuit (GMT)**
    - **En cause: un compteur 32 bits**
    - **2^{32} * 0,1 seconde = 13,6 ans depuis la conception du produit**
      - **http://isc.sans.edu/diary.html?storyid=9862**
  - **Un homme condamné pour piratage sur VoIP**
    - **Il a été arrêté après avoir été dénoncé par son ex-copine**
      - **http://www.itworld.com/print/121849**
  - **La NAT pour IPv6**
      - **http://sourceforge.net/projects/map66/**

Infos Unix

- **(Principales) faille(s)**
  - **Encore des failles énormes découvertes par Tavis Ormandy**
    - **(Mauvais) support de la variable LD_AUDIT par les binaires *setuid***
      - **http://seclists.org/fulldisclosure/2010/Oct/257**
      - **http://seclists.org/fulldisclosure/2010/Oct/344**
    - **Impact: élévation de privilèges locale**
  - **Faille dans le noyau Linux**
    - **http://git.kernel.org/?p=linux/kernel/git/stable/linux-2.6.32.y.git;a=commit;h=8816b5d01705e2c5c32bbf9e39e9aebad10b5dca**
  - **Faille dans l'implémentation du *globbing***
    - **Affecte: Solaris, *BSD, GNU Libc, etc.**
      - **http://securityreason.com/achievement_securityalert/89**
    - **Conduit à des exploitations possibles**
      - **Ex. serveurs FTP**

Infos Unix

- ProFTPd 1.3.x
  - Exécution de code à distance avant authentification
  - Faille introduite en corrigeant une autre faille
    - http://bugs.proftpd.org/show_bug.cgi?id=3521
    - http://www.zerodayinitiative.com/advisories/ZDI-10-229/
    - http://archives.neohapsis.com/archives/fulldisclosure/2010-11/0050.html
- Failles multiples dans PAM
    - http://www.certa.ssi.gouv.fr/site/CERTA-2010-AVI-530/CERTA-2010-AVI-530.html
- MySQL < 5.1.52
    - http://dev.mysql.com/doc/refman/5.1/en/news-5-1-52.html

Infos Unix

- **Support du protocole RDS par Linux**
  - **http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commitdiff;h=799c10559d60f159ab2232203f222f18fa3c4a5f**
- **XPDF**
  - **_Overflow_ divers**
    - **CVE-2010-3702**
    - **CVE-2010-3704**
- **Joomla! < 1.5.21**
  - **XSS divers**
    - **http://developer.joomla.org/security/news/9-security/10-core-security/322-20101001-core-xss-vulnerabilities.html**
- **Sympa < 6.1.1**
  - **http://www.certa.ssi.gouv.fr/site/CERTA-2010-AVI-505/CERTA-2010-AVI-505.html**

Infos Unix

- Autre

Failles

- **Principales applications**
  - **Plus de 80 failles dans les produits Oracle ce trimestre**
    - **Failles Java < 1.6.0_22**
      - **http://www.oracle.com/technetwork/topics/security/javacpuoct2010-176258.html**
    - **Exploits**
      - **http://skypher.com/index.php/2010/10/13/issue-18-oracle-java-applet-childre/**
      - **http://skypher.com/index.php/2010/10/13/issue-2-oracle-java-object-launchjnlp-docbase/**
      - **http://blog.mindedsecurity.com/2010/10/java-6u21-seven-issues-summary.html**
    - **Autres produits**
      - **http://www.oracle.com/technetwork/topics/security/cpuoct2010-175626.html**
    - **Exploits**
      - **http://www.appsecinc.com/resources/alerts/oracle/2010-03.shtml**
      - **http://www.bonsai-sec.com/en/research/vulnerabilities/oracle-virtual-server-agent-command-injection-0109.php**
    - **Note: Oracle 9 n'est plus supporté "en standard"**

Failles

- FireFox < 3.6.11
  - http://www.mozilla.org/security/known-vulnerabilities/firefox36.html#firefox3.6.11
  - Plusieurs failles intéressantes
    - MFSA 2010-72 Insecure Diffie-Hellman key exchange
    - MFSA 2010-71 Unsafe library loading vulnerabilities
    - MFSA 2010-70 SSL wildcard certificate matching IP addresses
    - MFSA 2010-69 Cross-site information disclosure via modal calls
    - MFSA 2010-68 XSS in gopher parser when parsing hrefs
    - MFSA 2010-67 Dangling pointer vulnerability in LookupGetterOrSetter
      - http://www.zerodayinitiative.com/advisories/ZDI-10-219/
    - MFSA 2010-66 Use-after-free error in nsBarProp
    - MFSA 2010-65 Buffer overflow and memory corruption using document.write
    - MFSA 2010-64 Miscellaneous memory safety hazards (rv:1.9.2.11/ 1.9.1.14)
  - Dont une faille trouvée par un enfant de 12 ans
    - http://www.mercurynews.com/san-jose-neighborhoods/ci_16401891

Failles

- ThunderBird < 3.1.5
  - Mêmes failles
    - http://www.mozilla.org/security/known-vulnerabilities/thunderbird31.html#thunderbird3.1.5
- FireFox < 3.6.12, ThunderBird < 3.1.6
    - http://www.mozilla.org/security/announce/2010/mfsa2010-73.html
    - http://bugix-security.blogspot.com/2010/10/firefox-exploitcve-2010-3765.html
  - Faille exploitée en "0day" sur le site du prix Nobel de la Paix …
    - http://community.websense.com/blogs/securitylabs/archive/2010/10/27/critical-vulnerability-in-firefox-browser.aspx
- Opera < 10.63
    - http://www.opera.com/docs/changelogs/windows/1063/

Failles

- RealPlayer (cf. bulletin pour les versions affectées)
  - http://service.real.com/realplayer/security/10152010_player/en/
  - ZDI-10-209, ZDI-10-210, ZDI-10-211, ZDI-10-212, ZDI-10-213
  - http://secunia.com/secunia_research/2010-13/
- WireShark < 1.4.1
  - http://www.wireshark.org/security/wnpa-sec-2010-12.html
- Chrome < 7.0.517.44
  - http://googlechromereleases.blogspot.com/2010/10/stable-channel-update.html
  - http://googlechromereleases.blogspot.com/2010/11/stable-channel-update.html
- BlackBerry Enterprise Server
  - Faille dans la conversion des fichiers PDF
    - http://www.blackberry.com/btsc/search.do?cmd=displayKC&docType=kc&externalId=KB24547
- Mac OS X < 10.5.8, < 10.6.3
  - Corrige des failles Java
    - http://support.apple.com/kb/HT4418
    - http://support.apple.com/kb/HT4417

Failles

- ShockWave Player < 11.5.9.615
  - 11 failles dont une exploitée en "0day" dans la nature
    - http://www.adobe.com/support/security/advisories/apsa10-04.html
    - http://www.exploit-db.com/exploits/15296/
  - Crédits:
    - binaryproof + anonymous / ZDI-10-227
    - Junaid Bohio / TELUS
    - Honggang Ren / Fortinet
    - Carsten Eiram / Secunia (x2)
      - http://secunia.com/secunia_research/2010-113/
      - http://secunia.com/secunia_research/2010-114/
    - Rodrigo Rubira Branco / Checkpoint (x4)
    - Anonymous / ZDI-10-228
  - Une autre faille … pas forcément facile à exploiter …
    - http://secunia.com/advisories/42112/

Failles

- Flash Player < 10.1.102.64
  - http://www.adobe.com/support/security/advisories/apsa10-05.html
  - http://blogs.adobe.com/psirt/2010/11/potential-issue-in-adobe-reader.html

  – Faille exploitée en "0day" dans la nature
    - http://contagiodump.blogspot.com/2010/10/potential-new-adobe-flash-player-zero.html
    - http://bugix-security.blogspot.com/2010/10/new-adobe-0day-bug-in-flash-player.html
    - http://blog.fortinet.com/fuzz-my-life-flash-player-zero-day-vulnerability-cve-2010-3654/
    - http://archives.neohapsis.com/archives/fulldisclosure/2010-11/0024.html
  – Corrigée une semaine plus tard dans Flash Player
    - http://www.adobe.com/support/security/bulletins/apsb10-26.html

  – Crédits
    - Tokuji Akamine / Symantec
    - Xiaopeng Zhang / Fortinet
    - Erik Osterholm / Texas A&M University
    - Matthew Scott Bergin / Smash The Stack & Bergin Pen. Testing
    - Will Dormman / CERT (x12)
    - Simon Raner / ACROS Security

Failles

- BIOS: la faille totale
  - http://dogber1.blogspot.com/2009/05/table-of-reverse-engineered-bios.html
- Double free dans Windows Mobile
  - Affecte: Windows Mobile 6.1 et 6.5
  - Exploit: exploitation via une vCard malformée
    - http://archives.neohapsis.com/archives/fulldisclosure/2010-10/0313.html
- HP Insight Manager
  - Téléchargement de fichiers arbitraires
    - http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c02548231
- Symantec IM Manager
  - ZDI-10-220, ZDI-10-221, ZDI-10-222, ZDI-10-223, ZDI-10-224, ZDI-10-225, ZDI-10-226
- SonicWall SSL-VPN
  - http://software.sonicwall.com/Aventail/KB/hotfix/10.0.5/clt-hotfix-10_0_5-003.txt

Failles

- Intel Baseboard Management Component (BMC) Firmware
  - Processeurs Xeon 5500 et 5600
    - http://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00026&languageid=en-fr
- Copieurs Xerox
  - "Déni de service" à distance
    - http://www.xerox.com/downloads/usa/en/c/cert_XRX10-004_v1.0.pdf
- FaceTime sur Mac OS X permet d'avoir tous les détails sur l'utilisateur
    - http://www.macnotes.net/2010/10/21/facetime-for-mac-a-serious-threat-for-your-apple-id/
- Backdoor dans le produit "IBM Rational Quality Manager and Test Lab Manager"
  - En fait un compte "admin/admin" par défaut dans Apache/Tomcat
    - http://www.zerodayinitiative.com/advisories/ZDI-10-214/
- Toutes les applications compilées avec Visual Studio + MFC sont vulnérables au "*DLL preloading*"
  - En cause: dwmapi.dll
    - http://blog.acrossecurity.com/2010/10/how-visual-studio-makes-your.html

Failles 2.0

- Advanced Evasion Threat
  - Réelle menace … ou nouvelle démonstration de l'inefficacité des IDS ?
    - http://www.antievasion.com/
  - Dommage que cette campagne soit orchestrée par un vendeur d'IDS !
  - Les réactions des concurrents
    - http://blogs.gartner.com/bob-walder/2010/10/20/storm-in-a-teacup-more-on-advanced-evasion-techniques-aet/
    - http://vrt-sourcefire.blogspot.com/2010/10/some-facts-about-advanced-evasion.html
- FireSheep
  - Le piratage sur les hotspots WiFi n'a jamais été aussi facile
    - http://codebutler.github.com/firesheep/

Failles 2.0

- Quelques sources de failles infinies
  - Les FRAMEs
    - http://lcamtuf.blogspot.com/2010/10/attack-of-monster-frames-mini.html
  - La GUI
    - http://lcamtuf.coredump.cx/ffpause/
  - Les Cookies
    - http://lcamtuf.blogspot.com/2010/10/http-cookies-or-how-not-to-design.html
- TechCrunch compromis
    - http://blog.seculert.com/2010/10/iranian-cyber-army-strikes-back.html

Failles 2.0

- Facebook
  - Le virus "Boonana" se propage sur Facebook
    - Originalité: virus "*cross-platform*", écrit en Java
      - http://nakedsecurity.sophos.com/2010/10/28/cross-platform-worm-targets-facebook-users/
  - Facebook passe à l'OTP par SMS
    - http://blog.facebook.com/blog.php?post=436800707130
  - Les options de vie privée dans Facebook ne servent à rien
    - Elles ne sont pas efficaces contre les applications !
      - http://online.wsj.com/article/SB10001424052702304772804575558484075236968.html
  - Des doutes sur le (futur) service "Facebook Places" également
    - http://www.cnil.fr/la-cnil/actu-cnil/article/article/facebook-places-en-questions-1/

Malwares et spam

- Qui a dit que les Honeypots étaient morts ?
  - Maintenant ils servent à attraper les "gentils" !
    - http://www.boingboing.net/2010/11/05/botmasters-include-f.html
- Les serveurs C&C de Bredolab saisis par la police néerlandaise
    - http://www.om.nl/actueel/nieuws-_en/@154338/dutch_national_crime/
  - Un message d'avertissement a été envoyé à tous les PC infectés, ce qui pose les habituelles questions d'éthique
    - https://www.waarschuwingsdienst.nl/Risicos/Virussen+en+malware/Ontmanteling+Bredolab.html
- Phone Creeper
  - Un logiciel d'espionnage pour mobiles, gratuit et performant !
    - http://forum.xda-developers.com/showthread.php?p=3977534
- Un vrai-faux "Microsoft Security Essentials" en circulation
    - http://blogs.technet.com/b/mmpc/archive/2010/09/01/rogue-msil-zeven-wants-a-piece-of-the-microsoft-security-essentials-pie.aspx
- Communication F-Secure
    - http://besmarterthanjohn.com/

Actualité (francophone)

- SSTIC 2011
  - Du 8 au 10 juin 2011
    - https://twitter.com/#!/sstic/status/27268820356
- Un nouveau centre de "super calcul"
    - http://www.enseignementsup-recherche.gouv.fr/cid53727/un-nouveau-centre-dedie-au-calcul-intensif-et-a-la-simulation-haute-performance.html
- Campagne "Internet Sans Crainte"
    - http://www.internetsanscrainte.fr/espace-jeunes/videos
    - http://www.2025exmachina.net/
- La Poste perd le monopole du recommandé électronique
    - http://www.france24.com/fr/20101022-conseil-detat-poste-perd-le-monopole-recommandes-electroniques
- 10% des adresses IP identifiées par HADOPI sont invalides
    - http://www.pcinpact.com/actu/news/60008-hadopi-volumetrie-identification-email.htm

Actualité (anglo-saxonne)

- Le rapport 2010 de la commission USCC en préparation
  - U.S.-China Economic and Security Review Commission (USCC)
    - http://news.cnet.com/8301-1009_3-20020461-83.html
- Le WiFi anglais est une passoire
    - http://www.ispreview.co.uk/story/2010/10/14/uk-report-exposes-poor-wifi-isp-security-and-potential-for-illegal-p2p-abuse.html
- Gemalto attaque Google pour violation de brevets
  - Ainsi que Motorola, Samsung et HTC
    - http://www.solutions-logiciels.com/actualites.php?actu=8395

Actualité (européenne)

- *Data Breach Notifications*
  - http://www.enisa.europa.eu/act/it/data-breach-notification/data-breach-notifications-in-europe-2013-the-way-forward
- Consultation sur le commerce électronique
  - http://www.laquadrature.net/fr/pourquoi-repondre-a-la-consultation-sur-le-commerce-electronique
- Exercice "Cyber Europe 2010"
  - http://www.enisa.europa.eu/media/press-releases/cyber-europe-20102019-cyber-security-exercise-with-320-2018incidents2019-successfully-concluded
- Interpol lance un outil de blocage des sites pédophiles
  - http://news.hostexploit.com/cyber-security-news/4575-interpol-launches-tool-to-block-online-access-to-child-abuse-material.html
- L'Allemagne lance "De-Mail"
  - Une transposition de la direction européenne sur la concurrence dans les services postaux
    - http://www.cidal.diplo.de/Vertretung/cidal/fr/__pr/actualites/nq/2010__10/2010__10__14__De__Mail__pm.html

Actualité (Google)

- Des primes pour les failles dans les applications Web de Google
  - http://googleonlinesecurity.blogspot.com/2010/11/rewarding-web-application-security.html
- Faille exploitable à distance dans le navigateur d'Android 2.0 et 2.1
  - Bon courage pour *patcher* tous les téléphones existants
    - http://www.exploit-db.com/exploits/15423/
- Contournement du verrouillage d'un téléphone Android
  - Affecte le Motorola Droid uniquement
    - https://theassurer.com/p/756.html
- Autre contournement du verrouillage
  - Mot de passe = "null"
    - http://www.onlineshoppingfree.com/2010/08/24/android-unlock/
  - Seul moyen de contourner un bug dans la procédure de recouvrement (!)
    - http://code.google.com/p/android/issues/detail?id=3006

Actualité (crypto)

- Vulnérabilité dans les systèmes de cryptographie quantique
  - http://www.bulletins-electroniques.com/actualites/64837.htm

Actualité

- Sorties logicielles
  - Metasploit 3.5
    - Avec une version "Pro" plus touffue que la version "Express"
  - EvilGrade 2.0
    - Avec plus de 60 systèmes de mise à jour supportés
      - http://www.infobytesec.com/developments.html
  - Secunia Vulnerability Intelligence Manager
    - http://secunia.com/blog/148/
- VMWare vSphere 4.0 certifié EAL4+
  - http://www.vmware.com/company/news/releases/common-criteria-certification-vsphere.html
- Le Cloud Amazon gratuit pendant 1 an
  - http://aws.amazon.com/free/
- Novell lance le portail d'information "Trusted Cloud"
  - http://www.trusted-cloud.com/

Actualité

- Turquie vs. BlackBerry
  - http://www.turkishpress.com/news.asp?id=359490
- Apache Harmony ne sera pas "certifié Java"
  - http://www.theregister.co.uk/2010/10/18/oracle_ibm_jcp_openjdk/
- La conférence 27C3 uniquement sur préventes
  - https://presale.events.ccc.de/accounts/sign_in
- ShmooCon a du mal à faire un site Web qui marche
  - https://www.shmoocon.org/news
- Secunia "racheté"
  - Entrée d'un fond d'investissement au capital
    - http://secunia.com/blog/145/
    - http://secunia.com/blog/146/

Actualité

- L'Inde développe son propre système d'exploitation "*closed source*"
  - 50 personnes pendant 1 an ???
    - http://economictimes.indiatimes.com/infotech/hardware/India-to-develop-its-own-futuristic-computer-operating-system/articleshow/6719490.cms

- La Russie aussi !
  - 3,5 millions d'euros pour adapter Fedora
    - http://www.lemonde.fr/technologies/article/2010/10/27/la-russie-veut-creer-son-propre-systeme-d-exploitation_1432068_651865.html

Fun

- **iOS 4 FAIL**
  - **http://www.clubic.com/smartphone/iphone/actualite-374744-iphone-faille-niveau-verrouillage-mot.html**
- **Double jailbreak pour l'iPad**
  - **http://hackaday.com/2010/10/10/new-a4-jailbreak-debacle-puts-the-brakes-on-for-ipad/**
- **Des salariés américains demandent le paiement des "heures BlackBerry"**
  - **http://www.lesechos.fr/journal20101102/lec1_competences/020889432783-blackberry-la-grogne-contre-les-heures-sup.htm**

Fun

- Reddit recrute … à sa manière
  - http://blog.reddit.com/2010/11/thank-you-mr-nast-may-we-have-another.html
- Victorinox continue avec son concours débile
  - http://secure-contest.victorinox.com/
- "The PHP Language Compiler for the .NET Framework"
  - http://phalanger.codeplex.com/
- Benoît Mandelbrot est mort

Questions / réponses

- Questions / réponses
- Prochaine réunion
  - Mardi 14 décembre 2010
- N'hésitez pas à proposer des sujets et des salles