APOGEE Communications

Rapport de Veille Technologique Sécurité N°114

Janvier 2008

Les informations fournies dans ce document ont été collectées et compilées à partir de sources d'origines diverses et publiquement accessibles: listes de diffusion, newsgroups, sites Web, ...

Ces informations sont fournies pour ce qu'elles valent sans garantie d'aucune sorte vis à vis de l'exactitude, de la précision ou de la qualité de l'information. Les URL associées à certains thèmes sont validées à la date de la rédaction du document.

Les symboles d'avertissement suivants seront éventuellement utilisés:


Site dont la consultation est susceptible de générer directement ou indirectement, une attaque sur l'équipement de consultation, voire de faire encourir un risque sur le système d'information associé.


Site susceptible d'héberger des informations ou des programmes dont l'utilisation est répréhensible au titre de la Loi Française.

Aucune garantie ne peut être apportée sur l'innocuité de ces sites, et en particulier, sur la qualité des applets et autres ressources présentées au navigateur **WEB**.

La diffusion de ce document est restreinte aux clients des services VTS-RAPPORT et VTS-ENTREPRISE

APOGEE Communications – Groupe DEVOTEAM
1, rue GALVANI
91300 Massy Palaiseau

Pour tous renseignements
Offre de veille: http://www.devoteam.fr/
Informations: vts-info@veille.apogee-com.fr

Au sommaire de ce rapport ...

Le mot de la rédaction …

La **CNIL** interpelle le gouvernement au sujet du risque posé par la communication d'informations par des entreprises françaises, ou étrangères établies en France, dans le cadre de certaines procédures en vigueur aux Etats-Unis. L'intitulé du second volet de la communication de la **CNIL** résume parfaitement la situation: «des incertitudes juridiques nombreuses pour des risques financiers et industriels réels».

http://www.cnil.fr/index.php?id=2379

Ce début d'année aura vu la mise en ligne par le Ministère de l'Industrie d'un site remarquable consacré à la protection de la propriété intellectuelle. Véritable mine d'informations, ce site dénommé '**Guide de la propriété intellectuelle dans les pôles de compétitivité**' est organisé autour de cinq volets traitant de la réglementation, des outils et de cas pratiques. Un site à conserver dans les signets de son navigateur.

http://www.industrie.gouv.fr/guidepropintel/

Le rapport annuel du **CLUSIF** sur la cybercriminalité a été mis en ligne début Janvier. On notera que quelques 28 pages sur les 168 du rapport sont consacrées aux problèmes émergents liés aux mondes virtuels. Si comme moi vous n'êtes pas (encore) adeptes de ces nouveaux environnements (*que reste-t-il de Lord British ou de Diablo*) la lecture de ces pages vous ouvrira d'autres horizons.

http://www.clusif.fr/fr/production/ouvrages/pdf/PanoCrim2k7-fr.pdf

Nous terminerons en recommandant la lecture du très instructif numéro 62 de la revue interne du **CNRS** entièrement consacré au chiffrement, aux outils associés et à leur mise en œuvre.

http://www.sg.cnrs.fr/FSD/securite-systemes/revues-pdf/num62.pdf

Bertrand VELLE

PRODUITS ET TECHNOLOGIES

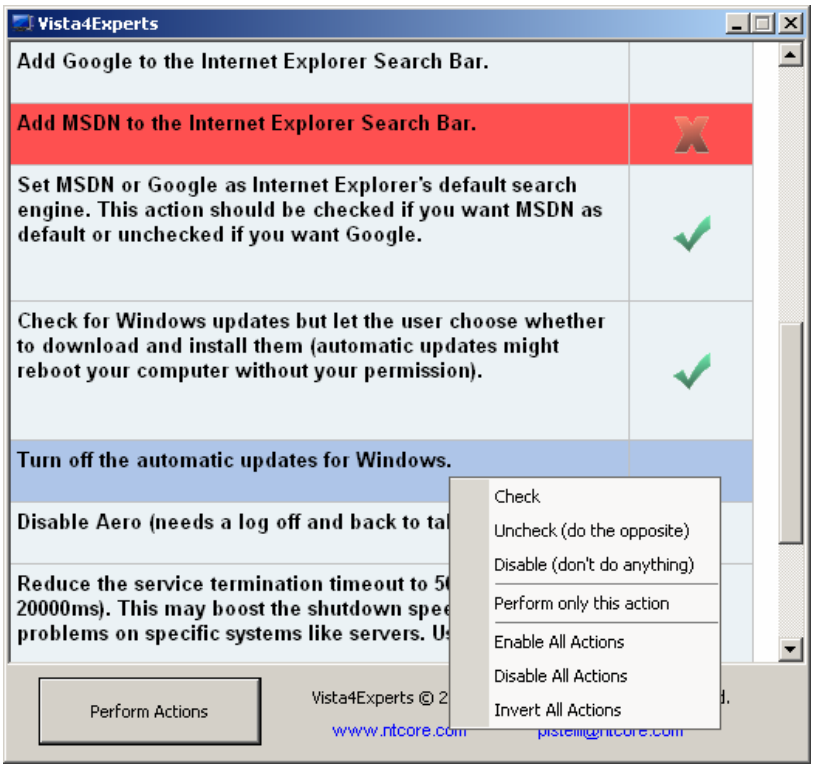
LES PRODUITS

SECURISATION

VISTA4EXPERTS V1.0.01

- **Description**

Géré par **Daniel Pistelli**, le site '**NTCore.com**' est très certainement connu de certains de nos lecteurs pour sa boîte à outils gratuite '**Explorer Suite**' laquelle intègre un outil de visualisation des processus et surtout **CFF Explorer**, un outil d'édition des en-têtes des exécutables Windows. Mais si l'on en croit un récent article sur son **Blog**, la notoriété de son site est désormais principalement due à la publication d'un outil dénommé **Vista4Experts** venant fort à propos aider les spécialistes à (re)configurer leur système **VISTA** sans avoir à recourir aux interfaces fermées proposées par Microsoft. Cet outil pourrait être comparé, du moins sur le plan des objectifs, aux **Power Toys** disponibles depuis les premières versions de Windows et encore pour la version **XP**.



Comme le dit l'auteur, **Vista4Experts** est surtout destiné aux personnes qui souhaitent utiliser **MSDN** ou **Google** comme moteur de recherche dans la barre de recherche d'Internet Explorer ou modifier l'action attachée au bouton Power, toutes ces petites modifications de l'environnement qui permettent de faire de celui-ci un outil parfaitement adapté à celui qui l'utilise.

Une rapide analyse de l'outil, écrit en langage C, confirme que toutes ces actions concernent la modification d'un ou plusieurs paramètres de la base de registre. On regrettera qu'un langage interprété n'a pas été utilisé ce qui aurait non seulement permis de vérifier l'absence de toute action 'anormale' mais aussi de rendre l'outil plus évolutif. Gageons que des outils concurrents ne vont pas tarder à faire leur apparition.

On notera à ce propos que rien n'interdit d'exécuter l'outil dans un environnement Windows différent de l'environnement cible – aucun contrôle n'est réalisé – mais les modifications effectuées pourront n'avoir aucun effet.

La version disponible à ce jour propose les actions suivantes:

- Add Google to the Internet Explorer Search Bar.
- Add MSDN to the Internet Explorer Search Bar.
- Always show the menu of Internet Explorer.
- Check for Windows updates but let the user choose whether to download and install them.
- Disable Aero (needs a log off and back to take place).
- Disable the File Indexing Service which might be time consuming.
- Disable the Security Center.
- Disable the User Account Control (UAC).
- Disable the Windows Sidebar.
- Disable Windows Defender's daily automatic scan.
- Google as homepage or unchecked if you want Live.
- Reduce the service termination timeout to 5000ms (default: 20000ms).
- Set Google or Live as Internet Explorer home page. This action should be checked if you want.
- Set MSDN or Google as Internet Explorer's default search engine.
- Show file extension even for known files.
- Switch to the classic view of the Control Panel.
- The start menu power button will shut down the system like in Windows editions before Vista.
- Turn off the automatic updates for Windows.

- When searching non-indexed locations, include system directories.

Il y aura cependant lieu de bien réfléchir avant de modifier – de manière parfaitement réversible fort heureusement - un comportement ou une option qui pourrait avoir un impact fort sur le niveau de sécurité du système.

▪ **Complément d'information**

http://ntcore.com/vista4experts.php - Présentation de l'outil
http://ntoskrnl.blogspot.com/ - Blog de Daniel Pistelli
http://www.microsoft.com/windowsxp/downloads/powertoys/xppowertoys.mspx - Les Power toys pour Windows XP

LES TECHNOLOGIES

ETUDES

CMU - TRAFFIC AGGREGATION FOR MALWARE DETECTION

▪ **Description**

Les résultats d'un rapport d'étude publié par le laboratoire de recherche en sécurité dit **CyLab** du l'université de **Carnegie-Mellon** pourraient bien intéresser les opérateurs et plus largement toutes les personnes ayant à faire face à un problème de compromission à large échelle par des codes malicieux communicants. Les auteurs y annoncent avoir trouvé une approche basée sur la métrologie des flux échangés aux frontières d'un réseau permettant de détecter la présence de systèmes compromis dans ce réseau quand bien même ceux-ci ne représenteraient que **0,0065%** de tous les systèmes présents sur ce même réseau (soit une machine compromise sur un réseau de 15384 machines non compromises).

Dénommé '**TĀMD**' - **T**raffic **A**gregation for **M**alware **D**etection, le sigle AMD n'ayant ici rien avoir avec les processeurs de la marque **AMD** - ce système s'appuie sur un ensemble d'algorithmes complexes permettant de mettre en évidence des caractéristiques communes aux flux échangés au bordure d'un réseau et de déterminer ainsi ce que les auteurs appellent un agrégat. Les auteurs montrent qu'un choix judicieux des algorithmes de détermination permet non seulement de déterminer des agrégats représentatifs de systèmes compromis mais aussi d'identifier de nouvelles formes de compromissions – notamment celles générées par des botnets – avec un très faible taux de faux positif.

Trois critères d'agrégation sont actuellement pris en compte:
1- l'existence d'une **destination commune**,
2- la présence d'une **similitude dans les données transportées**,
3- le partage d'un **même type de plateforme**.

Les auteurs font remarquer qu'aucun de ces critères pris indépendamment ne permettrait de distinguer un facteur pertinent mais que leur utilisation combinée permet d'obtenir d'excellents résultats. Sans remettre en doute cette conclusion – une certaine équipe chargée de la surveillance d'un très grand réseau dédié à la recherche utilise une approche similaire utilisant une métrologie **NetFlow** avec succès semble-t-il – nous nous posons la question de sa capacité à détecter les réseaux de machines compromises s'appuyant sur des mécanismes de communication de type **P2P** (mise en défaut du critère 1) ou pour lesquels les communications seraient **chiffrées** (mise en défaut du critère 2). Tous les exemples cités à ce sujet concernent des réseaux utilisant encore un canal de contrôle et de commande s'appuyant sur un centre nodal et un protocole non chiffré, en l'occurrence **IRC**.

Tout laisse pourtant à penser que les prochains **botnets** utiliseront des infrastructures de plus en plus complexes leur offrant à la fois **furtivité** et **résilience** et contre lesquelles il faudra bien disposer d'outils de détection efficaces. Le dernier numéro de la revue américaine '**;Login:**' proposait à ce sujet deux articles forts intéressants, coédités par deux spécialistes du sujet – **David Dittrich** et **Sven Dietrich** – proposant un état de l'art en matière de mécanismes de communication pour le premier article '**Command and Control Structures in Malware: From Handler/Agent to P2P**' et une analyse détaillée des deux plus grandes nuisances de ces dernières années pour le second article '**Analysis of the Storm and Nugache Trojans: P2P Is Here**'. Attention, seul le premier article est en accès libre.

Les règles de production et algorithmes de recherche de similitudes et d'analyse des destinations des flux sont détaillées dans le rapport technique, un mécanisme d'identification passive spécifique ayant été étudié, les mécanismes existants – '**nmap**' et '**p0f**' en particulier – ne convenant pas au format des données collectées dans le cas de la présente expérimentation. Les auteurs ont donc mis en place un mécanisme d'identification basé sur les caractéristiques du champ **TTL** – **T**ime **T**o **L**ive – permettant de caractériser de manière fiable le système d'exploitation ayant transmis le paquet contenant ce champ, ce mécanisme étant complété par une analyse des caractéristiques du trafic généré par ce même système d'exploitation: obtention de l'heure (protocole **NTP**), obtention d'une adresse (protocole **DHCP**), téléchargement de paquetages spécifiques à environnement ou depuis un site dédié à cet environnement (protocole **FTP**)… Une approche dont les avantages et inconvénients sont ensuite détaillés par les auteurs.

Le seuil de détection de 0.0065% qui pouvait paraître provenir d'une erreur de frappe a été établi par les conditions de validation expérimentale décrites en fin de rapport. Les auteurs ont utilisé le réseau de l'université – deux classes B et plus de 30 000 machines actives sur une période d'une heure - dans lequel ils ont inséré entre deux et huit machines compromises avec plusieurs variations de malwares, en l'occurrence **Bagle**, **IRCBot**, **MyBot** et **SdBot**. Soit un seuil de détection de 2/30000 dans le meilleur des cas. Le trafic aux bordures du réseau a été collecté six jours par semaine de 9h du matin à 3h de l'après-midi à l'aide de l'utilitaire '**Argus**' – quelques 5000 traces par seconde ! - puis traité avec les règles d'agrégation. Dans toutes les variantes des conditions de validation, les règles mises en œuvre ont permis d'identifier les machines compromises avec une très faible marge d'erreur.

Plusieurs agrégations considérées comme mineures par les auteurs ont été générées par du trafic anodin – probes **ICMP**, connections **SMTP** en time-out ou encore requêtes **HTTP** – mais aussi par des échanges non étudiés dus à du trafic de type **P2P** dont les auteurs considèrent qu'il s'agit d'échanges anodins…

Reconnaissons que, s'il est facile d'insérer quelques machines 'compromises' utilisant un mécanisme de communication 'classique' utilisant un serveur central sans compromettre l'ensemble du réseau, il devient plus difficile d'opérer en grandeur nature avec les dernières versions de certains codes, nous pensons particulièrement à **StormWorm** ou **Nugache**. Les résultats auraient pourtant été intéressants! Il nous faudra donc attendre qu'un laboratoire mette au point une simulation fiable de la propagation et du trafic généré par ces deux monstrueuses merveilles de technicité pour pouvoir valider, au moins sur le plan théorique, l'approche ici proposée.

Sommaire du rapport d'étude

- **Complément d'information**

http://www.cylab.cmu.edu/default.aspx?id=2387 - Press release
http://www.cylab.cmu.edu/files/cmucylab07017.pdf - Report

CMU - An Execution Infrastructure for TCB Minimization

- **Description**

Le laboratoire de recherche en sécurité dit **CyLab** de l'université de **Carnegie-Mellon** vient de publier les résultats de nouveaux travaux menés sur le thème de la certification de l'intégrité d'un code.

Ce rapport technique s'inscrit dans la continuité des travaux d'études innovants menés par le **CyLAB**. Ce dernier avait en effet publié l'année dernière les résultats d'une étude ayant permis de mettre au point un protocole interactif permettant de valider l'intégrité d'une application sensible avant son exécution sous l'intitulé '**PRISM: Enabling Personal Verification of Code Integrity, Untampered Execution, and Trusted I/O on Legacy Systems or Human-Verifiable Code Execution**' (Rapport N°109 – Août 2007).

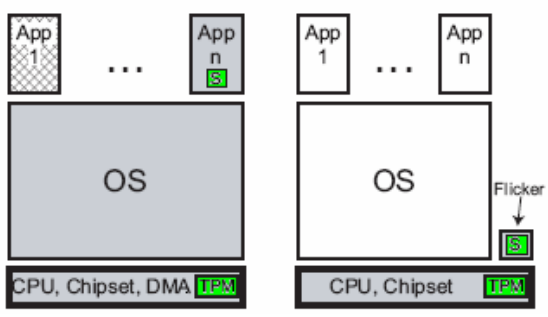
Une équipe du **CyLab**, constituée de chercheurs de **Carnegie Mellon** mais aussi de l'université de **Caroline du Nord** et de la société **Toshiba**, s'est ainsi donnée pour objectif d'exploiter les fonctionnalités de sécurité offertes par le module de sécurité **TPM** et les fonctionnalités de virtualisation intégrées aux derniers processeurs **Intel** et **AMD** pour créer un environnement d'exécution minimaliste et aisément vérifiable capable d'exécuter en toute sécurité un code sensible quand bien même certains composants logiciels – **BIOS**, **OS**… - de la plateforme seraient compromis.

Cet objectif est d'autant plus ambitieux qu'il impose que l'infrastructure mise en œuvre - dénommée **Flicker** – réponde à des exigences contraignantes vis-à-vis des interférences externes et, notamment, qu'aucun des codes chargés avant son activation dont le **BIOS** ne puissent interférer avec elle, ou superviser son fonctionnement.

Une telle infrastructure, appelée '**TCB**' - **T**rusted **C**omputing **B**ase – dans le jargon, est classiquement constituée d'un système autonome, disposant de sa propre capacité de calcul, physiquement protégé contre toutes tentatives d'intrusion et offrant une interface d'accès dédiée. Autant de mécanismes permettant de garantir que les données sensibles ne seront jamais exposées et que le code exécuté restera intègre.

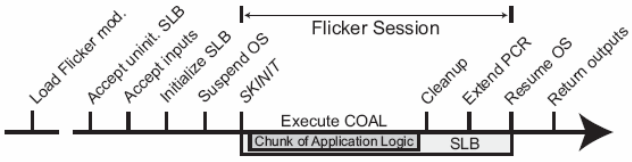
L'infrastructure **Flicker** s'appuie, elle, sur des capacités déjà présentes dans l'architecture du système hôte: une puissance de calcul offerte par le processeur du système hôte, des fonctions cryptographiques et de sécurité embarquées dans le composant inaltérable dit **TPM** (Trusted Platform Module) présent sur toutes les plate-formes récentes et, c'est là l'innovation, un mécanisme d'isolation tirant profit des fonctionnalités de virtualisation des processeurs récents.

Il est alors possible de concevoir un environnement d'exécution minimaliste n'ayant aucun lien avec l'environnement logique et matériel extérieur en dehors de l'interface avec le **TPM** dont le code pourrait être contenu dans une machine virtuelle.



En pratique, la robustesse de cet environnement sera directement liée à la capacité de cloisonnement offerte par son support, c'est-à-dire la technologie de virtualisation sous-jacente: **SVM** (Secure Virtual Machine) pour **AMD** ou **TXT** (Trusted eXecution Technology) pour **Intel**.

L'approche retenue pour l'infrastructure '**Flicker**' ne fait donc appel à la capacité de virtualisation que le strict temps nécessaire à l'exécution du 'bout' de code sensible ici appelé '**COAL**' - **C**hunk **O**f **A**pplication **L**ogic – dans une machine virtuelle créée au vol.



Dans le cas de la technologie de virtualisation testée - celle du processeur **AMD** - la création de cette machine virtuelle s'accompagne d'opérations spécifiques faisant appel aux fonctionnalités du **TPM**, les accès externes à la zone mémoire contenant le code d'initialisation de la machine étant par ailleurs verrouillés.

Un code de moins de 313 octets dit '**SLB Core**' assure les opérations de préparation de l'environnement virtuel, d'exécution du **COAL**, de nettoyage et de retour dans l'application.

Le rapport d'étude détaille les mécanismes qui ont été employés pour assurer le passage des paramètres d'entrée, la récupération des résultats et la validation de l'intégrité de ces derniers.
L'étude de l'impact sur les performances par rapport à une solution plus traditionnelle met en évidence l'influence du **TPM** et plus particulièrement de l'opération 'Unseal' qui permet de récupérer une donnée en vérifiant son intégrité laquelle pourra demander jusqu'à 400ms avec un **TPM** rapide ou de l'opération 'Quote' utilisée pour signer un bloc de données en utilisant une clef interne qui nécessite 940ms.

L'approche 'Flicker' est, de notre point de vue, celle de l'avenir car simple à mettre en œuvre par un développeur – un fichier d'inclusion, un gestionnaire de périphérique et quelques fichiers annexes – vérifiable – moins de 250 lignes de code constituant le chargeur '**SBL Core**' – et directement liée au processeur du système.

On pourra objecter que la robustesse des mécanismes de virtualisation proposés par **AMD** ou **INTEL** est régulièrement remise en cause ce à quoi l'on objectera qu'elle ne pourra que s'améliorer dans le futur conférant un réel intérêt à l'approche '**Flicker**'. Aucune information n'est cependant donnée dans le rapport d'étude concernant l'utilisation de cette approche, et ses performances, en environnement **INTEL**.

Nos lecteurs intéressés par les spécifications du **TPM**, véritable centre névralgique de la sécurité des **SI** à venir pourront parcourir le site du '**Trusted Computing Group**', l'organisation responsable de la normalisation de ce composant. Les spécifications de la dernière version – TPM V1.2 R103 – y sont librement téléchargeables.

- **Complément d'information**

http://www.cylab.cmu.edu/default.aspx?id=2388 - Press release
http://www.cylab.cmu.edu/files/cmucylab07018.pdf
https://www.trustedcomputinggroup.org/news/presentations/TCG_ESC_NTRU.pdf

INFORMATIONS ET LEGISLATION

LES INFORMATIONS

CONFERENCES

CCC - 24 CHAOS COMMUNICATION CONGRESS

- **Description**

Intitulée '**Volldampf voraus!**' – '**En avant à toute vapeur**' ou encore '**à plein pot**'– l'édition 2007 de la conférence '**Chaos Communication Congress**' s'est tenue du 27 au 30 décembre dernier avec quelques 102 présentations au programme. Il serait illusoire de tenter de résumer toutes les présentations dont certaines n'ont été données que dans la langue de **Goethe** ou dont le sujet n'a pas grand-chose à voir avec notre thème central d'intérêt: la sécurité des SI. Ne seront donc ici commentées que les présentations ayant attiré notre attention car traitant d'un sujet innovant ou d'actualité.

Face à la diversité des présentations et souhaitant proposer une liste 'exploitable' de toutes celles-ci, nous avons opéré un classement différent de celui proposé par les organisateurs de la conférence, en ne conservant que trois catégories sans tenir compte de l'existence d'un support ou de langue utilisée par l'orateur: les présentations ayant directement trait à la sécurité, celles ayant un intérêt culturel – du moins de notre point de vue et les autres présentations.

Ce tri s'est effectué sur la base d'une rapide lecture du sujet et des supports disponibles ou, le cas échéant, des vidéos. Toutes les présentations ont en effet été filmées et les vidéos sont disponibles sur le site **CCC**.

Thème 'Sécurité et Attaques'		
Community	After C: D, libd and the Slate project	Vladsharp
Culture	VX - The Virus Underground	SkyOut
Hacking	**10GE monitoring live!**	Arien Vijn
	A collection of random things	Ilja
	AES: side-channel attacks for the masses	Victor Muñoz
	AnonAccess	Otte, Heisrath
	Crouching Powerpoint, Hidden Trojan	Van Horenbeeck
	Current events in Tor development	Roger Dingledine
	Cybercrime 2.0 - Storm Worm	Thorsten Holz
	DNS Rebinding And More Packet Tricks	Dan Kaminsky
	From Ring Zero to UID Zero	sgrakkyu twiz
	Grundlagen der sicheren Programmierung	Tonnerre Lombard
	Hacking SCADA	Raoul "Nobody" Chiesa
	haXe: hacking a programming language	Nicolas Cannasse
	Inside the Mac OS X Kernel	lucy
	IPv6: Everywhere they don't want it	Jeroen Massar
	Just in Time compilers - breaking a VM	Peter Roland
	Konzeptionelle Einführung in Erlang	Strigler
	Latest trends in Oracle Security	Alexander Kornbrust
	Mifare part1 part2	Plötz, Nohl
	One Token to Rule Them All	Luke Jennings
	OpenSER SIP Server	Henning Westerholt
	Port Scanning improved	FX & Fabs
	Relay attacks on card payment: vulnerabilities and defences	Steven J. Murdoch
	Ruby on Rails Security	Jonathan Weiss
	Smartcard protocol sniffing	Marc-André Beck & all
	Unusual Web Bugs: A Web Hacker's Bag O' Tricks	kuza55
	Wireless Kernel Tweaking	Wunderlich
Lecture	To be or I2P	Jens Kubieziel
Making	Make Cool Things with Microcontrollers	Mitch
	Paparazzi - The Free Autopilot - Build your own UAV	Müller, Drouin (FR)
Science	Automatic memory management	Hannes
	Dining Cryptographers, The Protocol	Immanuel Scholz
	How to know what a text in an unknown language is about?	Martin Haase
	Quantum Cryptography and Possible Attacks	Christian & all
	Data Retention and PNR	Ricardo, Fontes
Society	NEDAP-Wahlcomputer in Deutschland	Kurz,Rieger

	Overtaking Proprietary Software Without Writing Code	Olivier Cleynen
	Tactics to hack the individual into the ICANN system	Muehlberg & all
	The demise of electronic voting in The Netherlands	Rop Gonggrijp
	TOR	Mittenzwei & all

Thème 'CutIture Sécuritaire'		
Community	Hacker Jeopardy	Stefan 'Sec' Zehl Ray
	Toying with barcodes	FX of Phenoelit
Hacking	<NO>OOXML - A 1 campaign Against Microsoft Office's broken standard	Benjamin Henrion
	A Spotter's Guide to AACS Keys	Peter Eckersley
	C64-DTV Hacking	Peter Fuhrmann
	Deconstructing Xbox 360 Security	Steil, Domke
	Desperate House-Hackers	Nils Magnus
	I know who you clicked last summer	Svenja Schröder
	Playstation Portable Cracking - How In The End We Got It All!	TyRaNiD
	Reverse Engineering of Embedded Devices	dash
	Security Nightmares 2008	Ron Frank Rieger
Making	OpenStreetMap, the free Wiki world map	Frederik Ramm
	Steam-Powered Telegraphy	Jens Ohlig
Science	Introduction in MEMS	Introduction in MEMS
	Modelling Infectious Diseases in Virtual Realities	floX
	Programming DNA	Drew Endy
	Simulating the Universe on Supercomputers	Mark Vogelsberger
Society	Digital Sustainability	Meike Richter
	Distributed campaigns for defending freedom in digital societies	J.Zimmermann (FR)
	EU Policy on RFID & Privacy	Andreas Krisch
	GPLv3 - Praktische Auswirkungen	Peter Voigt
	Meine Finger gehören mir	starbug
	Open Source Lobbying, tips from the trenches	Arjen Kamphuis
	The Arctic Cold War	Bicyclemark
	Wahlchaos	Markus Schneider
	What can we do to counter the spies?	Annie Machon

Thème 'Autre'		
Community	Building a Hacker Space	Lars, Ohlig
	Chaos Jahresrückblick	Frank Rieger & all
	The Role of Brilliant Deviants in the Liberalization of Society	Rose White
Culture	All Tomorrow's Condensation	Johannes Grenzfurthner
	Design Noir	ladyada
	Getting Things Done	Stephan Schmieder
	Rule 34 Contest	Andreas & all
	The image of computers in popular music	Johannes Grenzfurthner
Hacking	Anonymity for 2015: Why not just use Tor?	Len Sassaman
	Hamburger Wahlstift	Sven Übelacker & all
	Take the pain out of running a Bittorrent-Tracker!	Yxen, Erdgeist
Making	DIY Survival	Bre
	Elektronische Dokumente und die Zukunft des Lesens	Steini
	FeM-Streaming und Encoding	Sway Felix von Leitne
	Steam-Powered Telegraphy	Jens Ohlig
	The history of guerilla knitting	Rose White
Science	Absurde Mathematik	Dehghani
	Agenten des Bösen	Wolfgang Wippermann
	Analysis of Sputnik Data from 23C3	Tomasz Rybak
Society	23 Wege für Deine Rechte zu kämpfen	Beckedahl
	Das Panoptische Prinzip - Filme über die Zeit nach der Privatsphäre	Yvette Krause & all
	Der Bundestrojaner	Andreas Bogk
	Die Wahrheit und was wirklich passierte	Ron Frank Rieger
	Freifunkerei And a Do-It-Yourself society against the state	Gregers Petersen
	Hacking ideologies, part 2: Open Source, a capitalist movement	Tomislav Medak & all
	Hacking in the age of declining everything	Emerson
	Lieber Cyborg als Göttin	Cyworg
	Sex 2.0 - Hacking Heteronormativity	Florian Bischof
	Space Communism	Oona & all
	Spiel, Freude, Eierkuchen?	Rosengart, Fromm
	What is terrorism?	Anne Roth

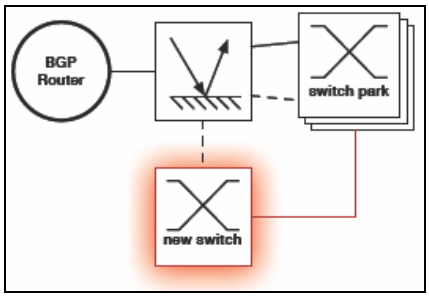
De ce véritable creuset à idées qu'est devenue cette conférence, idées dont certaines pourraient être taxées de

délirantes – on notera la présentation '**Steam-Powered Telegraphy**' expliquant comment remplacer le moteur électrique d'un bon vieux 'telex' par un moteur à vapeur (*que ne faut-il inventer pour exister dans ces univers parallèles ou décalés dont le courant **steampunk** est un excellent exemple*) - quelques présentations méritent une attention toute particulière pour leur qualité.

10GE monitoring live! — Ariën Vijn

Sous un titre quelque peu abscons, **Arian Vijn** se propose en fait de nous initier à la complexité de l'acquisition de données sur des réseaux à très haut débit, ici 10Gb/s, en nous amenant à constater les limitations inhérentes aux mécanismes proposés par les fournisseurs d'équipements.

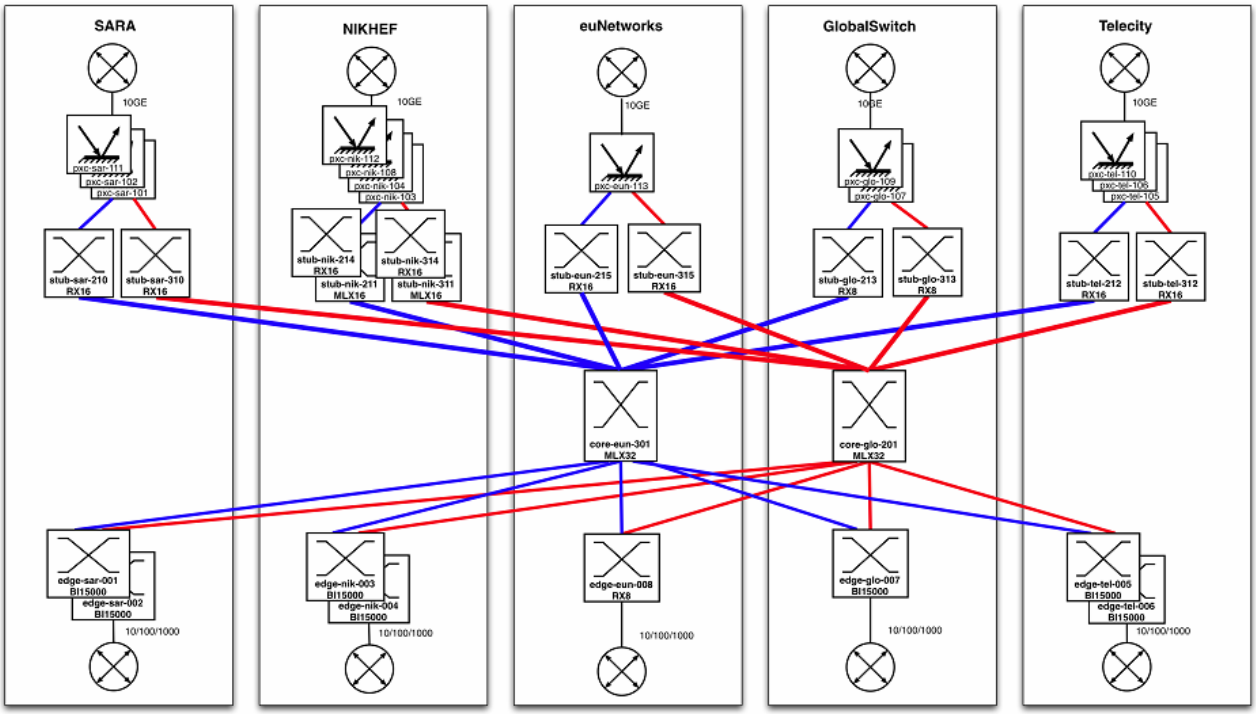
Pour illustrer son propos, l'auteur imagine une architecture d'accès sur un réseau haut débit constituée d'un accès fibre optique, d'un routeur **BGP**, d'un démultiplexeur optique et d'un banc de commutateurs.



Une architecture que le commun des mortels a bien peu de chance de rencontrer au quotidien mais dont l'intérêt est ici de montrer la difficulté qu'aura un exploitant à tracer et déboguer un problème tel que celui proposé par l'auteur: l'ajout d'un commutateur dans la ferme provoque des problèmes de performance.

L'approche classique consistera à utiliser les mécanismes de mesure et de surveillance embarqués dans le commutateur, mécanismes qui ne permettront pas toujours d'analyser les problèmes aux interfaces.

L'auteur affirme, et nous le croyons sur parole, que cette approche prendra des semaines faute de pouvoir disposer d'un recul suffisant et d'une vision globale du trafic. Aurions nous oublié de préciser que l'auteur travaille à l'**AMS-IX**, le centre d'interconnexion – ou 'Peering' – d'**Amsterdam**, lequel assure le transit et l'interconnexion de quelques 291 domaines autonomes de routage sur 499 ports et dont la plateforme d'interconnexion ressemble à l'exemple proposé … mais en plus compliqué encore. Nous ne résistons d'ailleurs pas au plaisir de reproduire ci-dessous leur cœur de réseau.



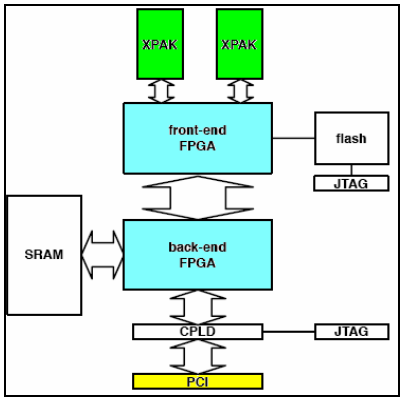
On peut dès lors imaginer le casse-tête auquel se trouvent confrontés les exploitants lors de l'apparition d'un défaut, et en particulier, si celui-ci n'est pas systématique car dépendant de paramètres externes non identifiés. L'étude d'un équipement d'acquisition et d'analyse dédié a donc été engagée par l'équipe de l'**AMS-IX**.

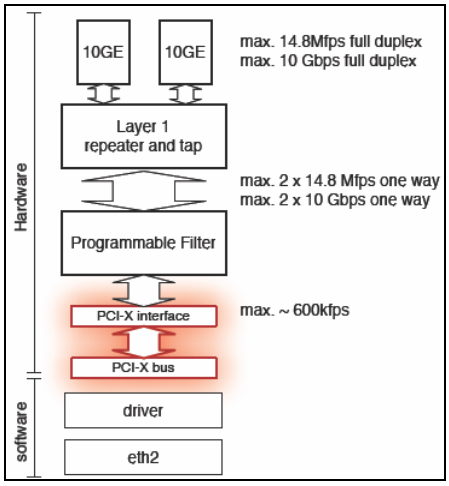
Une première solution étudiée consistait en une plateforme PC classique interfacée sur le port de recopie des commutateurs. A 10Gb/s, cette plateforme aurait à traiter dans le plus mauvais des cas – trames de 64 octets – quelques 14.8 millions de trames par seconde. Dans ces conditions, les tests menés ont démontré que cette solution ne permettait pas de traiter plus de 1.5 millions de trames par seconde. Un complément d'étude sur les mécanismes de recopie ont par ailleurs prouvés que, sur un commutateur **Foundry Networks de la série RX**, l'activation du mécanisme de recopie conduisait à perdre des trames – de 36% à 70% - au-delà d'un certain débit.

Comment alors disposer d'éléments de débogage fiables quand la seule collecte de ceux-ci influence le comportement de l'équipement surveillé et par là même, l'ensemble du comportement du réseau !

Les auteurs se sont donc tournés vers la seule solution viable: l'acquisition des données directement au niveau de la ligne optique et leur traitement par le biais d'un équipement spécifique.

L'utilisation d'une carte dédiée a été envisagée dont le rôle serait d'assurer, outre la capture des trames, le filtrage sélectif de celles-ci selon des critères reprogrammables.





Dans ces conditions, un bus d'interface normalisé – **PCI** e**X**tended - peut être utilisé sans aucune crainte de voir celui-ci saturé par le volume des données remontées comme cela était le cas avec la première solution étudiée.

Pour éviter d'avoir à développer une telle carte, les auteurs se sont tournés vers la société **Force 10 Network** laquelle a conçu une carte d'acquisition pour ses propres équipements de sécurité – **IDS**, **IPS**, surveillance et interception légale – de **la série P10**. Un logiciel embarqué a été écrit qui vient remplacer celui de la société Force 10 Network, logiciel qui a été optimisé pour le besoin. Cette carte est intégrée sur une plateforme PC classique fonctionnant sous **LINUX**, des modules de gestion assurant l'interface entre les applications et la carte.

Les règles de filtrage sont exprimées sous la forme d'expressions conformes à la syntaxe '**tcpdump**' qui sont ensuite mises en forme pour être traitées par les mécanismes implémentés par des **FPGA** – circuits contenant des blocs de logique reprogrammable - dans la carte. Le lecteur intéressé pourra découvrir en fin de présentation le déroulement de la logique de traitement d'un filtre **tcpdump** '**not ether src 00:01:02:03:04:05**' lequel assure le rejet de toutes les trames ayant pour source l'adresse MAC 00:01:02:03:04:05.

http://www.force10networks.com/products/pseries.asp
http://events.ccc.de/congress/2007/Fahrplan/attachments/1005_24C3_AV.pdf

Playstation Portable Cracking - How In The End We Got It All! — TyRaNiD

Si un prix d'excellence devait être distribué, cet article le remporterait haut la main. Il contient en effet tous les ingrédients pour en faire un best-seller et réponds à toutes les questions que nous nous posions sur la genèse d'une attaque réussie, en l'occurrence, le cassage de l'ensemble des mécanismes de protection de la célèbre console de jeu **PSP** conduisant à faire de celle-ci, une plateforme ouverte et aux performances remarquables.

Conçue pour n'autoriser que l'exécution d'applications dûment certifiées par **Sony -** principalement des jeux enregistrés sur un support de type **DVD** non reproductible - cette console a rapidement fait l'objet de modifications lui permettant d'exécuter une image logique stockée dans la carte mémoire de la console. Plusieurs évolutions successives ont conduit à la mise à disposition de firmwares 'modifiés' de plus en plus performants et ouverts dont les célèbres versions '**OE'** produites par **Dark Alex** et '**M33**' du groupe de 'bidouilleurs' éponyme.

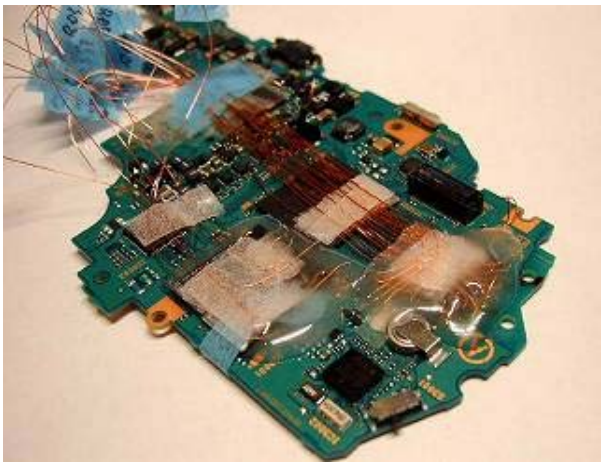
Après de multiples péripéties, **Dark Alex** ayant rejoint le groupe **M33**, les fanatiques de cette console disposent désormais d'un fabuleux système alternatif, stable et dont la mise à jour n'a jamais été aussi aisée, à condition toutefois de l'avoir installé une première fois. Et c'est ici la partie la plus difficile de l'exercice puisque cette installation ne peut intervenir qu'à la faveur d'une faille exploitable dans l'un des jeux disponibles pour la version du système couramment installée sur la console, le système livré avec les consoles mises sur le marché étant régulièrement mis à jour par Sony pour fermer les failles découvertes. Jusqu'à peu, la technique consistait à exploiter la 'bonne' faille dans l'optique d'installer une ancienne version du système – 'downgrader' le système dans le jargon – en tenant compte de la révision du matériel puis à construire le système alternatif à partir de cette version. En cas d'erreur, la sanction était immédiate, la console devenant aussi inutile qu'une brique.

Ayant 'brické' une console il y a trois mois à la suite d'une erreur de manipulation, nous découvrions un fabuleux utilitaire permettant d'imposer le chargement du code de démarrage de la console depuis la carte mémoire en lieu et place de la mémoire flash interne. L'altération du mode de démarrage se trouve être conditionnée par le contenu d'une mémoire embarquée dans les batteries d'origine, mémoire contenant entre autre chose le numéro de série de la batterie. La réinsertion d'une batterie modifiée à partir d'une console fonctionnelle - batterie dénommée '**Pandora Battery**' par les inventeurs de la méthode - et d'une carte mémoire externe contenant un firmware valide permet alors à la console 'brickée' de revenir à la vie par rechargement du firmware dans la mémoire flash.

La question qui se posait alors à nous était celle de l'origine de cet outil miraculeux dont nous pensions qu'il ne pouvait que provenir des services de maintenance de '**Sony**'. Qui d'autre aurait pu découvrir que la manipulation d'une donnée dans une zone de la mémoire embarquée dans la batterie pouvait influencer le mode de démarrage de la console ?

La présentation de '**TyRaNid**' répond à cette question, et à bien d'autres, en mettant en évidence le cheminement entre la découverte d'un point d'entrée involontairement laissé en place par **Sony** dans la toute première version de son firmware jusqu'à la découverte du mécanisme d'activation d'un démarrage en mode dégradé et la diffusion non voulue du code par l'un des membres de l'équipe.

On y apprend que la sécurité du système aurait pu être préservée si **Sony** n'avait été pressé par le temps pour sortir sa console en même temps que son concurrent conduisant à un relâchement des procédures et à la diffusion d'une version en cours de développement. La sécurité du système était alors, à jamais, doublement compromise: par l'ouverture d'un accès simple au code du système et par l'existence même d'une version ouverte dont il suffisait de trouver un moyen permettant de la recharger pour reprendre immédiatement le contrôle du système.



Ajoutons à cela l'existence d'une grossière erreur dans la logique de traitement des erreurs lors de la vérification d'un condensé conduisant à réduire l'espace de test de 2^128 à 4*2^32 essais.

Le reste n'est qu'une question de patience, d'une certaine dose de génie et en dernier recours de l'utilisation a bon escient des outils d'ingénierie désormais à la portée de tous. Il suffit pour s'en convaincre de lire le support de présentation.

On retiendra de cette aventure que l'on ne peut accélérer les développements sans risquer de mettre à jamais en péril la sécurité de l'ensemble du système mais aussi que, pour des raisons purement industrielles, les équipements actuels disposent toujours d'un accès dérobé permettant d'automatiser la validation de leur bon fonctionnement en sortie de la chaîne, et le cas échéant, de reprogrammer le code embarqué.

http://events.ccc.de/congress/2007/Fahrplan/attachments/1040_psphacking.odp

Toying with barcodes — FX

Proposée par **FX**, membre du célèbre groupe **Phenoelit**, cette intervention porte sur un concept que tout le monde connaît – les codes barres – mais dont on découvre avec bonheur la diversité au fur et à mesure de la lecture du support de présentation.

L'auteur commence par un rapide historique du développement de cette forme de stockage optique d'information développé dés 1948 et nous propose un portrait de famille de 13 codes de la première génération, dite '**codes 1D**' en référence au codage n'utilisant qu'une seule dimension.

Quatre codes de la seconde génération sont ensuite présentés tous caractérisés par un encodage utilisant la surface du support, codes en conséquence dénommés '**codes 2D**'. Ces codes, véritables pictogrammes, utilisés depuis plusieurs années dans les milieux industriels pour la traçabilité des produits, sont désormais connus du grand public car désormais utilisés par les sociétés de colisage et de 'billeterie électronique'.

Ils permettent en effet le stockage d'un volume conséquent de données avec une excellente fiabilité de relecture et sans nécessiter l'utilisation d'un équipement d'impression dédié. Dans bien des cas, une simple imprimante 300dpi suffira à produire un code 2D exempt de toute erreur de relecture. Nous ouvrons à ce sujet une parenthèse pour rappeler l'existence d'un outil extraordinaire conçu par l'auteur du non moins extraordinaire débogueur **OllyDBG**. Dénommé '**PaperBack**', cet outil permet la sauvegarde de données – en particulier le code source de ses applications – par l'impression en 600dpi d'un bitmap représentatif de ce code. L'auteur annonce une capacité d'encodage d'environ 500Ko par feuille A4. L'extraction du code est réalisée par un programme d'analyse et nécessite un scanner offrant une résolution d'au moins 900dpi. Une idée géniale utilisant un procédé proche de celui des codes barres 2D.

La présentation de **FX** se poursuit par la description de l'offre actuelle en matière de logiciels d'encodage et d'équipements de lecture et de décodage. La qualité des codes récents, et plus encore, celle des équipements de lecture facilite la reproduction d'un code barre avec les 'moyens du bord' sans altération de sa lisibilité.

L'auteur décrit plusieurs exemples de contrefaçon de codes barres ayant été exploités avec succès: passe d'accès au bar d'un hôtel, ticket d'accès à un parking privatif, multiples remboursements d'une même consigne. Ces fraudes ont exploité différentes vulnérabilités dans le cycle d'utilisation du code barre conduisant à pouvoir rejouer le code. L'auteur passe en revue quelques-unes des failles qu'il a pu mettre en évidence dans des services quotidiennement utilisés par le grand public allemand:

- Architecture technique interdisant toute invalidation d'un code déjà utilisé,
- Utilisation d'un code prédictible et aisément altérable,
- Contrôle d'intégrité insuffisant ou ne vérifiant que la bonne structure des données,

La facilité avec laquelle un quelconque code peut être copié, quand bien même les données ne pourraient être altérées, ouvre la porte à une fraude assez aisée à mettre en œuvre quand le dit code n'est corrélé avec aucune autre information. L'auteur cite quelques cas de mise en application: l'un dans le cas d'un contrôle de présence basé sur la seule présentation du code barre permettant ainsi à un employé de sortir de l'entreprise en endossant l'identité d'un autre, l'autre permettant de sortir de l'inventaire un portable totalement différent de celui-ci qui devait sortir en remplaçant simplement les codes barres correspondant au numéro de série, au numéro d'inventaire et à l'adresse **MAC** ceci sans changer l'identification lisible associée à chacun de ces éléments.

La présentation se termine sur la description de quelques attaques plus complexes qui, pour certaines, s'appuient sur la sophistication grandissante des lecteurs de code. Ces derniers peuvent devenir vulnérables à des attaques classiques dont des débordement de buffer ou l'injection de code **SQL** dans les bases d'inventaire, le code d'exploitation étant ici tout simplement imprimé !

On lira avec plaisir l'analyse de l'encodage utilisé par les services postaux Suisse et Américain et celui des cartes d'embarquement de la Lufthansa. L'auteur annonce cependant ne pas encore avoir réussi à découvrir la structure des codes utilisés par la poste Allemande ou encore par les services des douanes Américains !

La société Française **ASK** a probablement trouvé une excellente solution à tous ces problèmes avec son produit '**C.Ticket**', un ticket papier classique combiné avec une puce **RFID**, une approche qui sera utilisée pour les tickets d'accès aux jeux olympique de **Pékin**.

http://www.phenoelit-us.org/
http://www.ask.fr/fr/products_and_services/c_ticket.html
http://events.ccc.de/congress/2007/Fahrplan/attachments/1055_toying_with_barcodes.pdf

How to know what a text in an unknown language is about ? — Martin Haase

Martin Haase est linguiste. Il enseigne à l'université de Cologne. Sa présentation tente de répondre à un problème couramment rencontré lors de balades sur l'Internet: en quelle langue cette page est-elle rédigée ou ce texte est-il écrit ?

Le lecteur restera cependant sur sa faim, la présentation ne faisant qu'effleurer un sujet complexe pour lequel une recherche sur le moteur de recherche de citation '**CiteSeer**' permet d'identifier de très nombreux travaux. Parmi ceux-ci, la méthode décrite dans la présentation et proposée en 1976 par **Norman Ingle**, un linguiste. Celui-ci a établi une liste de mots de un ou deux caractères en y associant un index permettant d'identifier la ou les langues qui les utilisent. Une approche simple, efficace et aisément automatisable s'il n'y avait l'écueil de la représentation 'numérique' de certains caractères ou symboles.

L'auteur nous propose cependant une intéressante liste de quatre outils publiquement accessibles:

- **TexCat** 76 langages
- **LangUID** 65 langages
- **LanguageGuesser** 40 langages
- **PolyGlot3000** 441 langages

Il termine sa présentation par la mise en pratique de la loi de **Zipf** laquelle stipule que les mots les plus fréquents sont les plus courts et contiennent bien moins d'information lexicale que les mots les plus longs bien moins fréquents. Le linguiste occasionnel pourra tirer profit de cette loi empirique, dont Wikipedia nous apprend qu'elle a été généralisée par le mathématicien Français **Benoit Mandelbrot**, en extrayant d'un texte inconnu les mots les plus longs et en recherchant leur signification par le biais d'un moteur de recherche classique. Un exemple de mise en œuvre est proposé avec un texte écrit en Samoan.

http://events.ccc.de/congress/2007/Fahrplan/attachments/1026_LingHack-Slides.pdf
http://events.ccc.de/congress/2007/Fahrplan/attachments/1025_LingHack-Paper.pdf
http://www.cis.upenn.edu/~jcreynar/sdair96.pdf/sibun96language.pdf

Mifare: Little Security, Despite Obscurity — Plötz, Nohl

Conçue par la société **Philips**, la technologie de cartes sans contact dite '**Mifare**' est incontestablement un très grand succès. Elle est utilisée dans de multiples domaines par des professionnels mais aussi par des particuliers, son coût étant très abordable et des kits de prise en main étant disponibles. Une carte **Mifare** a même été distribuée avec le magazine d'électronique **Elektor** dans un numéro consacré à la réalisation d'un lecteur de badges **RFId**. Ces cartes se distinguent par deux familles, l'une constituée de cartes à mémoire dites **Mifare Classic** n'offrant qu'un espace de stockage allant de 64 octets à un peu moins de 4Ko, l'autre par des cartes à microprocesseurs offrant toutes les fonctionnalités attendues des cartes dites 'à puce'.

Les auteurs de la présentation se sont donc intéressés à la sécurité de la première version

> Crypto unit: The field proven CRYPTO1 stream cipher of the Mifare Classic family ensures a secure data exchange

dont Philips a toujours affirmé qu'elle offrait un haut degré de protection contre la copie, un algorithme non divulgué étant utilisé pour assurer l'authentification et la génération de la clef de chiffrement des échanges. Dénommé **CRYPTO1**, cet algorithme est codé dans la logique des cartes et dans le composant associé embarqué dans les lecteurs compatibles **MIFARE**.

Disposant de moyens conséquents mais disponibles dans tout bon laboratoire universitaire en l'occurrence celui de l'université de Virginie, ils ont attaqué le problème selon deux approches:

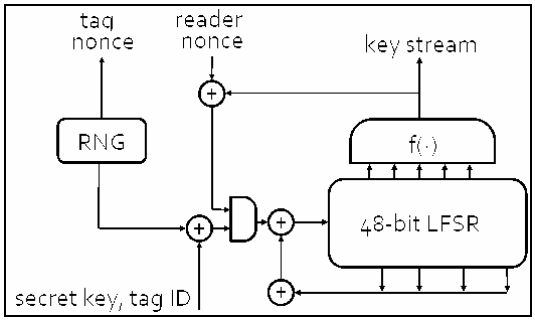
- analyse de type **boîte noire** où la seule observation des réponses à des stimuli contrôlés doit permettre de déterminer la nature du contenu de la boîte et d'en comprendre le fonctionnement,
- analyse de type **boîte blanche** où le contenu de la boîte est révélé et son analyse doit permettre d'en comprendre le fonctionnement.

La première approche nécessite de disposer d'une carte **MIFARE**, d'un lecteur compatible **MIFARE** (un **OpenPCD**) et d'un émulateur de carte (un **OpenPICC**) lequel permet d'espionner les échanges – données et déroulement temporel - entre le lecteur et la carte – moins de €200 au total. Un équipement d'enregistrement dénommé analyseur logique sera aussi nécessaire dont le coût va de €200 à €1000 selon les fonctionnalités embarquées.

Un schéma d'authentification en trois passes est ici utilisé qui s'appuie sur la connaissance de l'identifiant de la carte ou 'Tag ID', d'une clef secrète – laquelle n'est jamais transmise hors de la carte et sur une valeur aléatoire ou 'nonce' générée de part et d'autre. Un grand nombre d'échanges d'authentification a ainsi pu être collecté qui a permis de mettre en évidence une certaine régularité dans l'aléa transmis par la carte. Une analyse plus poussée a alors conduit à découvrir que cette valeur dépendait directement du temps écoulé entre la mise sous tension de la carte et le moment de la génération de l'aléa.

Les auteurs ont ensuite étudié la robustesse du mécanisme d'authentification en s'appuyant sur la méthode dite du 'bit flipping' qui consiste à observer les résultats d'un calcul d'authentification en modifiant un ou plusieurs bits bien choisis dans les données d'entrée, en l'occurrence la clef secrète et l'identifiant de la carte. La fonction de mélange de ces deux données s'est avérée être un simple OU exclusif – ou XOR – permettant aux auteurs d'affirmer qu'il leur était possible de déterminer un couple identifiant/clef valide pour un quelconque identifiant avec la seule connaissance d'un premier couple identifiant/clef valide !

La seconde approche, menée en parallèle, nécessite d'avoir à disposition le matériel requis pour extraire le composant d'une carte, éliminer la couche de passivation pour enfin pouvoir accéder à l'empilement des couches électroniques le constituant.



Les auteurs ont ainsi pu mener avec succès une rétro analyse de la logique de l'algorithme d'authentification et de chiffrement. Bien qu'aucun détail précis n'ait été encore révélé sur la fonction ici utilisée, celle-ci prend la forme d'un classique registre à décalage bouclé (ou **LSFR** – Linear Feedback Shift Registers) de 48bits utilisant d'après certaines indiscrétions 20 points de rebouclage ou '**tap**' dont les sorties sont ensuite filtrées pour ne conserver que le nombre utile de bits.

Le générateur aléatoire – 16 bits - apparaît alors immédiatement être le second point de faiblesse. Que la valeur utilisée lors d'une authentification puisse être imposée et toute la sécurité de la technologie **MIFARE Classic** tombe sous réserve toutefois de connaître le polynôme générateur du **LFSR** et la fonction de réduction. Les auteurs ont non seulement démontré qu'il était possible de contrôler cette valeur en maîtrisant le temps écoulé entre la mise sous tension et l'engagement de la première phase d'authentification mais aussi que ce générateur utilisait un **LSFR** de période 65535 et dont le polynôme [16,14,13,11] est celui de l'exemple proposé à la rubrique '**Fibonacci** LFSRs' de l'encyclopédie **Wikipedia**.

Que le lecteur se rassure, la conception de **Crypto1** remonte à plus de 10 ans donc bien avant que cet article ait été écrit. On notera d'ailleurs que le polynôme générateur de l'exemple proposé par Wikipédia à beaucoup changé: [17,15,1] en août 2003, [16,5,3,2] en avril 2005 pour arriver à [16,14,13,11] le 14 décembre 2005, la modification ayant été faite depuis une adresse dynamique localisée à Doncaster en Angleterre, donc a priori sans rapport avec l'affaire qui nous intéresse ici.

Les auteurs terminent leur analyse en suggérant l'existence d'une dernière vulnérabilité intrinsèque sans toutefois détailler le gain potentiel en terme de réduction de l'espace d'attaque. Ils considèrent cependant qu'une clef doit pouvoir être trouvée par recherche exhaustive en moins d'une semaine avec une architecture de cassage d'un coût inférieur à $100. L'architecture de **Crypto1** semble avoir été optimisée pour les performances au détriment de la robustesse.

http://www.nxp.com/acrobat_download/other/identification/m001052.pdf
http://events.ccc.de/congress/2007/Fahrplan/attachments/1049_CCC-07-Mifare-v2.pdf
http://events.ccc.de/congress/2007/Fahrplan/attachments/1051_24c3-mifare-henryk-ooo.pdf

Port Scanning improved - New ideas for old practices — FX & fabs

Sans cette présentation, on aurait pu croire que tout avait été dit sur cette technique consistant à identifier un équipement caché derrière une adresse IP en inventoriant les services actifs sur cette adresse. Cet art semblait avoir été porté à son apogée, du moins sur la place publique par **Fyodor**, l'auteur du célèbre outil '**nmap**'.

FX et **Fabs** nous prouvent qu'il n'en est rien en nous démontrant l'inefficacité de certains des algorithmes d'optimisation mis en œuvre dans '**nmap**' tout en présentant les différentes améliorations qu'ils ont testé et intégrés dans leur propre outil dénommé '**PortBunny**'.

Ils répondent tout d'abord à la question qu'il conviendrait bien plus souvent de se poser avant qu'un développement Open Source se proposant d'offrir une n^{ième} version d'un outil ou d'une application ne soit engagé.

De leur point de vue, il peut être intéressant – et même parfois nécessaire – de réinventer la roue lorsqu'un logiciel ne répond plus aux exigences actuelles ou quand les évolutions dans l'environnement d'utilisation l'imposent. Cependant, et c'est de notre point de vue une excellente analyse de la situation, la réécriture d'une application ne peut s'engager sans une réflexion préalable prenant en compte la capacité de l'équipe à réellement terminer le projet: un outil fonctionnel bien qu'imparfait sera toujours meilleur qu'un outil répondant à tous les besoins mais non terminé se plaisent à dire les auteurs.

Plus largement, ces derniers suggèrent d'aborder le développement avec les principes suivants en tête:

- Définir ses propres exigences fonctionnelles et s'y tenir quoiqu'il advienne sans tenter de contenter le monde entier,
- Ne pas tenir compte des exigences auquel répondait le développement existant. La portabilité n'est pas toujours requise pas plus que certaines des fonctionnalités proposées dans le contexte d'une nouvelle version,
- Eviter de se référer au(x) code(s) existant(s) afin de garder la tête claire et être capable de penser différemment. Il sera toujours possible de se référer au(x) code(s) existant plus tard.

Ces trois principes sont applicables à toutes les formes de développement qu'il s'agisse d'une nouvelle itération d'un projet tiers ou d'un nouveau palier fonctionnel d'un projet interne.

En ce qui concerne le projet '**PortBunny**', les auteurs se sont donnés comme objectif de disposer d'un outil de sondage de port destiné aux professionnels de l'audit et des tests d'intrusion, lesquels privilégieront la fiabilité et la rapidité au détriment de la portabilité, de la capacité à inventorier l'intégralité d'un réseau ou de fonctionnalités décoratives.

L'outil idéal permettra ainsi de déterminer, sur un ou plusieurs réseaux, la liste des systèmes dont le port **TCP/XYZ** est actif avec une méthode de détection simple (**TCP SYN**) sans perdre de temps avec des méthodes complexes n'apportant que peu de plus-value au regard de la perte de temps (la méthode **XMAS TCP** est explicitement visée) et sans même s'intéresser au protocole UDP (le sondage des port UDP est considéré par les auteurs comme une approche négative, c'est-à-dire n'apportant aucune information utile aux interfaces d'un système correctement sécurisé).

On le voit, les spécifications de '**PortBunny**' ne reprennent qu'un tout petit sous-ensemble de celles de '**nmap**' en ne conservant que les fonctionnalités strictement utiles dans un monde où, désormais, l'essentiel n'est plus d'inventorier tous les ports actifs d'équipements non sécurisés par défaut mais bien de cibler certains services dans le contexte d'une infrastructure réseau déjà correctement sécurisée.

Nous laisserons au lecteur le soin de lire le support de présentation pour prendre connaissance des techniques qui ont été utilisées pour optimiser dynamiquement la vitesse de sondage en tenant compte des différents goulots d'étranglement. Les performances obtenues sont, dans bien des cas, identiques si ce n'est meilleures que celle de '**nmap**', le facteur de gain tournant autour de 1.5 dans la majorité des cas pour atteindre 80 dans le cas du sondage de tous les ports d'un système distant dont les accès sont filtrés. Certaines améliorations n'ont cependant pu être obtenues qu'au détriment de l'intégration du moteur de sondage dans le noyau du système d'exploitation, un système LINUX, conduisant à la création du premier '**Linux-kernel-based port-scanner**'.

http://nmap.org/
http://www.recurity-labs.com/portbunny/portbunny.html
http://events.ccc.de/congress/2007/Fahrplan/attachments/1059_24c3PortBunnySlides.pdf

- **Complément d'information**

http://events.ccc.de/congress/2007/Fahrplan/ - Agenda des présentations

ITSI – SECURITY WORKSHOP 2008

- **Description**

L'**ETSI** a mis en ligne les supports des présentations effectuées à l'occasion du 3ième Security Workshop qui s'est tenu du 15 au 16 janvier à **Sophia Antipolis**. Nous proposons ci-dessous la liste des interventions avec un lien direct sur le support associé.

Introduction	
Keynote speech from the European Commission	Achilleas Kemos
ETSI Security Activities Overview	Charles Brookson
ENISA Activities in Security	Elisabetta Carrara
Sécurité des mobiles	
3GPP Security hot topics: LTE/SAE and Common IMS	Valtteri Niemi
Update on Security, Fraud thefts and Operators' initiatives in GSM and 3G	James Moran
IETF Security standardization activities	Hannes Tschofenig
Initiative de sécurité avec la CEN/CENELEC	
Cost-effective authentication and integrity of electronic invoices	Nick Pope
ESCoRTS: A European network for the Security of Control and Real-Time Systems	Alberto Stefanini
CEN Anti-Counterfeiting Workshop	Nadine Ruhle-Niestroy
Interception légale	
Lawful Interception and Data Retention standardization activities	Scott Cadzow
Secure, verifiable & intelligible audit logs to support computer forensics in LI	Elena de la Calle Vian
Lawful Interception of VoIP in Highly Decentralised Systems	Jan Seedorf
Nouveaux défis	
Trusted Computing and Trusted Computing Group	Claire Vishik
Producing and maintaining Standards for Emergency Communications	Jean-Pierre Henninot
ETSI TC related activities: STF 318 (REM) and XAdES interoperability event	Riccardo Genghini
Cartes à mémoire	
Developments within the ETSI Smart Card Platform Group	Klaus Vedder
Secure Internet Connectivity with the Internet Smart Card	Walter Hinz
ETSI Smart Card Platform WG: USSM, Secure Channel & Confidential Applications	Ilario Macchi
Secure UICC Hardware Platforms	Gerd Dirscherl
Normalisation internationale	
ICT Security Standards Roadmap: an Update	Mike Harrop
Global Cybersecurity: the role of International Standards	Solange Ghernaouti
Global Standards Initiative on Identity Management (IdM-GSI)	Scott Cadzow
Architecture and Privacy Issues for Biometric-Based Identity	Jean-Paul Lemaire
Sécurité des NGN	
NGN Security standards for Fixed-Mobile Convergence	Judith E. Y. Rossebø
VoIP, NGN and DoS: Attack Scenarios, Detection and Prevention	Dorgham Sisalem
PSTN/ISDN Emulation Subsystem (PES) within a NGN	Steve Covey
Comparison of the work of different SDOs regarding UC/SPIT with a demonstrator	Thilo Ewald

Cryptographie	
Standardization of Quantum Technologies and Cryptography: FP6 Integrated Project	Thomas Langer
A Compact and High-Speed Cipher Suitable for Limited Resource Environment	Taizo Shirai

- **Complément d'information**

http://portal.etsi.org/securityworkshop/ - Programme du workshop

http://portal.etsi.org/docbox/Workshop/2008_SECURITYWORKSHOP - Support des présentations

WIFI

TU-DARMSTADT – ATTACKS ON THE WEP PROTOCOL

- **Description**

S'il n'y a désormais plus aucun doute sur la réelle solidité du protocole **WEP** utilisé pour assurer la confidentialité des transmissions sur les réseaux sans-fils **IEEE 802.11**, il n'en reste pas moins que celui reste encore très employé, bien souvent pour des raisons pratiques: les particuliers ayant investis dans un équipement **WiFi** refusant de devoir encore dépenser pour le remplacer par un équipement a priori similaire.

L'intégration de l'équipement d'accès dans l'offre des **ISP** permet heureusement de garantir un renouvellement du parc installé, les '**box**' proposées disposant désormais de la dernière version du protocole **WAP**, la seule actuellement encore exempt de problèmes de sécurité. Un facteur pourra encore freiner la migration vers ce protocole, l'existence de périphériques imposant encore l'utilisation de versions antérieures: consoles de jeux, systèmes embarqués dédiés…

Une étude publiée dans le cadre d'une thèse présentée à l'université de Darmstadt propose un très intéressant état de l'art des attaques connues sur le protocole **WEP**. Une nouvelle classe d'attaque dite '**PTW**' du nom des auteurs – **Pyshkin**, **Tews** et **Weinmann** - y est par ailleurs détaillée.

Nous nous permettons de reproduire ci-dessous, la table des matières de cette étude de plus de 125 pages qui méritera de figurer en bonne place dans la liste des documents de base de la sécurité. Nous avons en effet particulièrement apprécié la qualité de la mise en page et la présence des nombreux schémas explicatifs accompagnant des formules mathématiques pour le moins rébarbatives.

- **Complément d'information**

http://eprint.iacr.org/2007/471.pdf - These

ENISA

ENISA - LA REVUE

- **Description**

Le dernier numéro de l'année 2007 de la revue '**ENISA Quarterly**' est paru début Janvier et a pour thème principal la sûreté des logiciels.

Pour clore cette année 2007, le directeur exécutif de l'**ENISA** propose, en introduction, un rapide tour d'horizon des événements marquants en mettant l'accent sur les actions menées en fin d'année dont notamment l'organisation de nombreux ateliers de travail et la publication de trois prises de position: sur les réseaux de machines Zombies, sur les réseaux de réputation et sur les réseaux sociaux (Rapports N°113 et 114 de Novembre et Décembre 2007).

Le programme de travail pour l'année 2008 intitulé '**ENISA driving for impact**' portera sur trois axes référencés **MTP** (**M**ulti-Annual **T**hematic **P**rogrammes) eux-mêmes organisés en unités de travail ou **W**ork **P**ac**K**age ('**WPK**') à savoir:

MTP / WKP	Effort	Budget
1. Improving resilience in European e-Communication networks	2008	2008
1.1 Stock taking and analysis of national security regimes to ensure security resilience of public communication networks	7.0hm	€200 000
1.2 Analysis of measures deployed by operators on resilience of public communication networks	10.5hm	€90 000
1.3 Analysis of existing technologies enhancing resilience of public communication networks	9.5hm	€100 000
2. Developing and maintaining co-operation models	2008	2008
2.1 Co-operation platform for Awareness Raising Community	14.0hm	€50 000
2.2 Security competence circle and good practice sharing for CERT communities	14.0hm	€120 000
2.3 Supporting the faster take up of interoperable eIDs in Europe	6.0hm	€80 000
2.4 European NIS good practice Brokerage	10.5hm	€160 000
3. Identifying emerging risks for creating trust and confidence	2008	2008
3.1 Framework for assessing and discussing emerging risks	7.5hm	€180 000
3.2 Position Papers	6.0hm	€100 000
	85.0hm	€1 080 000

Une action préparatoire - ou **PA** (**P**reparatory **A**ction) – a par ailleurs été inscrite à ce même programme:

PA / WKP	Effort	Budget
1. Building information confidence with micro enterprises	2008	2008
4.1 Analysing micro enterprises needs and expectations	4.5hm	€30 000
4.2 Assessing risk management process for micro enterprises	4.0hm	€80 000
	8.5hm	€110 000

Le lecteur désireux d'en savoir plus sur ce programme 2008 pourra lire avec intérêt le document fondateur de 43 pages intitulé '**WORK PROGRAMME 2008 – Build on Synergies – Achieve Impact**'.

Le sommaire de ce numéro de la lettre de l'**ENISA** consacré, rappelons-le à la sécurité des logiciels (ou devrions nous plutôt traduire à **la création de logiciels surs**), est reproduit ci-dessous:

A Word from the Executive Director
A Word from the Editor
A Word from the Experts
Cycles of Software Crises
The Whys and Hows of Assuring Secure Software
Technology Leaders Tackle Software Assurance
The 10 Most Common Sins of Software Developers
Security Skills of Software Developers
Leading the Way to More Secure Software
Providing Assurance for Security Software – Insights into the Common Criteria
From our own Experts
ENISA Position Papers
Towards an EISAS
Food for Thought
Stop Using the Traffic Analogy
ENISA Short News

Quelques articles méritent d'être mis en avant.

Cycles of Software Crises - How to avoid insecure and uneconomic software

Signé par **Markus Bautsch**, représentant des consommateurs au comité de direction de l'**ENISA**, cet article pose dès les premières lignes toute la problématique induite par le développement logiciel: s'il est difficile de trouver les

mesures adéquates pour assurer la production de logiciels sécurisés, il est a contrario assez simple de définir les propriétés et caractéristiques d'un logiciel non sécurisé. Les termes '**Secure**' et '**Insecure**' seront ici à prendre dans leur acceptation la plus large incluant les propriété de **fiabilité** et de **sûreté de fonctionnement**.

L'auteur aborde ensuite ce qui peut apparaître comme étant le problème de fond, celui de l'utilisation de langages de programmation n'intégrant pas ou peu de fonctionnalités de protection ou de garde-fous.

L'exemple classiquement cité est celui du langage '**C**' dont il est indiqué qu'il est encore utilisé dans des domaines où la sûreté de fonctionnement est une exigence première. Le monde de l'automobile est explicitement mentionné dans l'article lequel propose un tableau comparatif des fonctionnalités liées à la fiabilité offertes par quatre langages classiques (**CP** désigne ici le Component Pascal). On regrettera qu'une fois encore, le langage **ADA** soit purement et simplement passé sous silence.

Comparison of example programming languages

	C / C++	CP	Java	C#
Publication	1972/1985	1994	1995	2001
Structured syntax	no	yes	no	no
Simplicity and regularity	no	yes	no	no
Cyclic imports impossible	no	yes	no	no
Static objects	yes	yes	no	yes
Only simple implementation inheritance	no	yes	no	yes
Full module safety	no	yes	no	yes
Full type safety	no	yes	yes	yes
Automatic and mandatory garbage collection	no	yes	yes	yes
Dynamic loading	no	yes	yes	yes

Ouvrons ici une parenthèse pour rappeler que le principal défaut du langage 'C', et de son extension objet - le langage 'C++' - est de laisser au programmeur le soin de gérer l'allocation mémoire des types complexes de données avec le risque qu'une erreur d'allocation ne conduise à un dysfonctionnement de l'application. Faire porter toute la faute sur le langage serait oublier que l'architecture sous-jacente a elle aussi un rôle fondamental à jouer en pouvant offrir une dernière barrière de confinement permettant de limiter les risques de propagation d'une faute.

Citons par exemple, l'organisation de la pile de certains processeurs laquelle interdit l'écrasement de l'adresse de retour d'une fonction, et donc la possibilité de détourner – involontairement ou non - le flot d'exécution ou encore l'architecture mémoire séparant physiquement les bus d'exécution et de données.

Ignorer les spécificités de l'architecture sous-jacente, système d'exploitation et processeur, conduira inéluctablement à des problèmes aux limites et ceci quelque soit le langage utilisé. Nombreux sont ainsi les exemples de programmation proposés qui, utilisant des langages évolués, suggèrent d'affecter dans une variable l'intégralité des données issues de la lecture d'un fichier ou d'une requête SQL. Le bon fonctionnement d'une telle méthode aux limites du système dépendra pour une bonne part de l'implémentation du langage sur l'architecture cible mais aussi du bon usage par ce langage des fonctionnalités de gestion de la mémoire offertes par le système sous-jacent. En dernier recours, il sera de la responsabilité du programmeur de gérer proprement les cas d'exception.

Fermons maintenant cette parenthèse en rejoignant la prise de position de l'auteur lequel considère que la meilleure approche dans le domaine de la fiabilisation des logiciels consistera à s'appuyer sur des environnements de développement – et pas simplement sur un langage - dotés de toutes les fonctionnalités de protection et sur des outils permettant de garantir la génération d'un **code fiable et réutilisable** ainsi que l'absence de toute forme de programmation à risque.

La réutilisation, maître mot des développements à venir, n'a de sens qu'à la condition de disposer de codes, ou d'objets offrant la capacité d'être aisément vérifiables par l'environnement d'exécution - dit **PCC** (Proof-Carrying Code) - libérant ainsi le développeur d'avoir à se préoccuper de la sécurité de telle méthode ou de tel module. La seule contrainte résiduelle sera d'avoir à utiliser des outils et un environnement d'exécution qualifiés.

L'auteur précise que ce type d'approche est à l'étude notamment via le projet '**Mobius**' - **MOBI**lity, **U**biquity and **S**ecurity – piloté par l'**INRIA** et auquel il participe. Ce projet a pour objectif l'intégration d'une capacité d'auto-validation du code **Java** embarqué et exécuté sur des plates-formes mobiles compatibles **MIDP**.

http://mobius.inria.fr/twiki/bin/view/Mobius

Providing Assurance for Security Software – Insights into the Common Criteria

Rédigé par **David Ochel**, consultant pour '**AtSec**' une société spécialisée dans l'évaluation de sécurité, ce court article a pour principal mérite de positionner les contraintes liées au développement de logiciels sécurisés – au sens 'classique' du terme - dans le contexte des critères communs d'évaluation ou **CCSec**.

La version 2.3 de ces critères a été adoptée par l'ISO en tant que norme internationale sous référence **ISO/IEC 15408:2005**. L'auteur de l'article référence cependant la toute dernière version – **la version 3.1** – mais il s'agit probablement ici d'une erreur ou de la volonté d'anticiper sur la prochaine révision de la norme **15408**.

Les critères communs reconnaissent sept niveaux de confiance, ou **E**valuation **A**ssurance **L**evel, identifiés **EAL1** (niveau faible) à **EAL7** (niveau très élevé) qui permettront d'attester de la conformité d'un produit aux exigences de sécurité et de développement définies pour le niveau de confiance obtenu.

En pratique, l'évaluation porte sur un périmètre précis dit 'cible de sécurité' ou **TOE** (Target Of Evaluation) dont on vérifiera qu'il respecte tous les critères définis pour le niveau visé par le demandeur de l'évaluation.

Rappelons encore que les éléments de preuve devant être apportés par le développeur dépendront du niveau d'évaluation visé, le code source n'étant pas analysé dans le cas des trois premiers niveaux.

La norme définit six classes de critères, dites classes d'assurance, qui couvrent l'ensemble du cycle de vie du produit et au sein de chacune de ces classes, des familles de critères à respecter. Pour chacune de ces familles, le niveau d'analyse ira en croissant avec le niveau de confiance visé par l'évaluation.

On notera encore qu'il est parfaitement possible d'évaluer un produit à un niveau donné en sélectionnant pour certains composants des exigences supérieures à celles imposées pour ce niveau. On parlera alors de niveau augmenté, l'annotation '+' accolée au niveau de confiance étant alors utilisée.

Cette approche est parfaitement bien résumée par le tableau ci-contre extrait de l'article et modifié pour mettre en évidence le niveau 'charnière' **EAL4**.

CC 3.1								
Assurance class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Development	ADV_ARC		1	1	1	1	1	1
	ADV_FSP	1	2	3	4	5	5	6
	ADV_IMP				1	1	2	2
	ADV_INT					2	3	3
	ADV_SPM						1	1
	ADV_TDS		1	2	3	4	5	6
Guidance documents	AGD_OPE	1	1	1	1	1	1	1
	AGD_PRE	1	1	1	1	1	1	1
Life-cycle support	ALC_CMC	1	2	3	4	4	5	5
	ALC_CMS	1	2	3	4	5	5	5
	ALC_DEL		1	1	1	1	1	1
	ALC_DVS			1	1	1	2	2
	ALC_FLR	(ALC_FLR subactivities optional at all EALs)						
	ALC_LCD			1	1	1	1	2
	ALC_TAT				1	2	3	3
Security Target evaluation	ASE_CCL	1	1	1	1	1	1	1
	ASE_ECD	1	1	1	1	1	1	1
	ASE_INT	1	1	1	1	1	1	1
	ASE_OBJ	1	2	2	2	2	2	2
	ASE_REQ	1	2	2	2	2	2	2
	ASE_SPD		1	1	1	1	1	1
	ASE_TSS	1	1	1	1	1	1	1
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	2	3	3	4
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_VAN	1	2	2	3	4	5	5

Ce niveau est en effet couramment ciblé par les composants de sécurité dont les puces des cartes à mémoire, les produits classiques de sécurité étant, pour leur part, bien souvent actuellement évalués au niveau **EAL2+**, voir **EAL3+**.

Le niveau **EAL4** marque aussi la limite dans l'accord de la reconnaissance des certifications entres les 24 membres du **CCRA** – Common Criteria Recognition Arrangement – au nombre desquels figure la **France**. Ces membres s'organisent en deux groupes complémentaires:

- les membres conduisant les évaluations et produisant des certificats dits '**Certificate Authorising**' members: Australie et Nouvelle Zélande, Canada, France, Allemagne, Japon, République de Corée, Pays-Bas, Norvège, Espagne, Royaume-Uni et Etats-Unis,
- et les membres consommateurs dits '**Certicate Consuming**' members: Autriche, république Tchèque, Danemark, Finlande, Grèce, Hongrie, Inde, Israël, Italie, Malaisie, Singapour, Suède et Turquie.

Les limitations de l'approche **CC** sont parfaitement résumées dans l'article. En faisant abstraction du fait qu'aucune évaluation ne permettra jamais d'atteindre un niveau de confiance absolu, du moins dans un temps raisonnable et avec une énergie limitée, le problème le plus difficile à solutionner dans le contexte économique actuel est celui de la portée de la certification, celle-ci étant déclarée valide pour tout produit dans une configuration identique en tout point à celle du produit ayant été certifié. Qu'une modification soit effectuée, pour mineure qu'elle puisse être, et la certification ne sera plus valide. Cette contrainte, acceptable il y a encore une décennie, devient rédhibitoire dans un monde en évolution permanente où le cycle de vie d'un produit se réduit de jour en jour et dans lequel la réutilisation des composants se borne bien souvent à copier et adapter un code source.

L'auteur suggère de s'adapter à cet état de fait, et de prendre en compte les limitations de cette approche au titre de la gestion du risque. L'utilisation d'un produit certifié, avec une cible de sécurité éventuellement réduite, permettrait de recentrer l'effort sur les points qui ne seraient pas, ou plus couverts, par l'évaluation. L'auteur cite ainsi le choix Cornélien auquel serait confronté le responsable de sécurité dans le cas de l'application d'un correctif de sécurité sur un produit évalué et la logique de prise de décision qui s'ensuit. Entre deux maux, il faudra choisir le moindre: appliquer le correctif et perdre la certification ou mettre en œuvre les mesures externes permettant de risque latent.

Il s'agit là d'un exemple intéressant et d'une analyse fort pertinente mais pour laquelle l'auteur semble avoir oublié: 1- que le commun des mortels sera incapable de déterminer l'impact de l'application de ce correctif sur la fonction de sécurité ayant été évaluée et 2- que la découverte d'une vulnérabilité qui impacterait la fonction de sécurité ayant été évaluée remettrait implicitement en cause le niveau de confiance ayant été attribué voire la qualité de l'évaluation!

Un problème de ce genre a d'ailleurs été mis en évidence dernièrement, non pas dans le cadre des évaluations **CC** mais dans le cadre du programme américain de certification FIPS **CMVP** (**C**ryptographic **M**odule **V**alidation **P**rogram): l'application d'un correctif critique sur le composant '**FIPS Object Module v1.1.1**' intégré dans le paquetage **OpenSSL** et certifié **FIPS 140-2** en Juin 2007 impliquait la perte de cette certification.

La note d'information du 29/11/2007 associée à ce correctif stipulait d'ailleurs que toutes les informations requises concernant ce correctif avaient été transmises au laboratoire chargé de l'évaluation **FIPS 140-2** au **NIST** pour approbation. Les choses semblent avoir été rapidement menées dans ce cas précis puisque la version **v1.1.2** du module était publiée sur le site d'**OpenSSL** le 1er décembre avec la mention **FIPS** dans le nom du paquetage.

Quelques incohérences subsistent pourtant. Ainsi aucune annonce n'a officiellement confirmé la certification de cette nouvelle version ni sur le site **OpenSSL** ni sur la page consacrée aux produits et modules certifiés maintenue par le **NIST** laquelle mentionne toujours la version v1.1.1 tout en indiquant une mise à jour au 30/11/2007.

Tout ceci confirme, si besoin est, la difficulté rencontrée pour passer de la théorie à la pratique dans un système en perpétuelle mouvance.

Bytes	Timestamp	Filename
3269831	Dec 1 00:25:33 2007	openssl-fips-1.1.2.tar.gz (MD5) (SHA1) (PGP si
3354792	Oct 19 10:36:16 2007	openssl-0.9.8g.tar.gz (MD5) (SHA1) (PGP sign)
3357445	Oct 11 20:31:40 2007	openssl-0.9.8f.tar.gz (MD5) (SHA1) (PGP sign)
3341665	Feb 23 13:58:19 2007	openssl-0.9.8e.tar.gz (MD5) (SHA1) (PGP sign)
3303943	Feb 23 13:57:08 2007	openssl-0.9.7m.tar.gz (MD5) (SHA1) (PGP sign)
3315566	Sep 28 14:09:22 2006	openssl-0.9.8d.tar.gz (MD5) (SHA1) (PGP sign)
3294357	Sep 28 14:08:07 2006	openssl-0.9.7l.tar.gz (MD5) (SHA1) (PGP sign)
3313857	Sep 5 11:04:33 2006	openssl-0.9.8c.tar.gz (MD5) (SHA1) (PGP sign)
3292692	Sep 5 11:04:30 2006	openssl-0.9.7k.tar.gz (MD5) (SHA1) (PGP sign)
3279283	May 4 15:21:31 2006	openssl-0.9.8b.tar.gz (MD5) (SHA1) (PGP sign)
3290510	May 4 15:21:16 2006	openssl-0.9.7j.tar.gz (MD5) (SHA1) (PGP sign)
3280907	Oct 15 00:37:24 2005	openssl-0.9.7i.tar.gz (MD5) (SHA1) (PGP sign)
3271435	Oct 11 12:37:49 2005	openssl-0.9.8a.tar.gz (MD5) (SHA1) (PGP sign)
3287019	Oct 11 12:36:35 2005	openssl-0.9.7h.tar.gz (MD5) (SHA1) (PGP sign)
3259550	Jul 5 21:19:24 2005	openssl-0.9.8.tar.gz (MD5) (SHA1) (PGP sign)
3132217	Apr 11 17:21:51 2005	openssl-0.9.7g.tar.gz (MD5) (SHA1) (PGP sign)
3104957	Mar 22 20:23:13 2005	openssl-0.9.7f.tar.gz (MD5) (PGP sign)

Open Source Software Institute Administrative Office P.O. Box 547 Oxford, MS 38655 USA -John Weathersby TEL: 601-427-0152 FAX: 601-427-0156	**OpenSSL FIPS Object Module** (Source Content Version: openssl-fips-1.1.1.tar.gz; Resultant Compiled Software Version: 1.1.1) *(When built, installed, protected and initialized as specified in the provided Security Policy. Appendix B of the provided Security Policy specifies the complete set of source files of this module. There shall be no additions, deletions or alterations of this set as used during module build. All source files, including*	Software	02/06/2007-11/30/2007

http://www.commoncriteriaportal.org/public/expert/index.php?menu=2

- **Complément d'information**

http://www.enisa.europa.eu/doc/pdf/publications/enisa_quarterly_12_07.pdf
http://www.enisa.europa.eu/pages/02_01_press_2007_11_21_wp_2008.html - Annonce du programme de travail 2008
http://www.enisa.europa.eu/doc/pdf/management_board/decisions/enisa_wp_2008.pdf - Détail du programme de travail

ENISA – WHO IS WHO - EDITION 2008

- **Description**

L'**ENISA** a publié la mise à jour de son annuaire des différents services gouvernementaux chargés de traiter les problèmes liés à la sécurité des SI dans les différents états membres de l'Europe. Celui-ci est disponible sous la forme d'un document de 230 pages – soit 121 pages de plus que la toute première édition datant de décembre 2005 (Rapport N°89 – Décembre 2005).

Cette nouvelle édition du ''**Who is Who Directory on Network and Information Security**' pourra s'avérer bien utile pour identifier le service vers qui se tourner dans l'hypothèse d'un problème ayant pour source l'un des états membres de l'Europe.

Concernant la France (page 63), sont toujours référencés:
- pour les services du Premier Ministre:
  la **DCSSI**, le **CFSSI** (le centre de formation de la DCSSI), le **CERTA**,
- pour le Ministère de l'Intérieur:
  l'**OCLCTIC**,
- pour le Ministère de l'Economie, des Finances et de l'Industrie:
  la **DGME**/**SDAE** (Direction Générale de la Modernisation de l'Etat /Service pour le Développement de l'Administration Electronique)

- **Complément d'information**

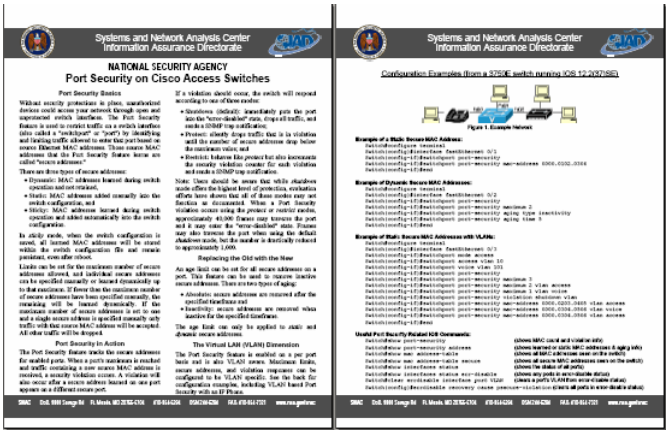
http://www.enisa.europa.eu/doc/pdf/deliverables/who_is_who_dr_20080121.pdf

SECURISATION

NSA - PORT SECURITY ON CISCO ACCESS SWITCHES

- **Description**

Publié par la **NSA** et intitulé '**Port Security on Cisco Access Switches**', ce mémento technique de 2 pages décrit de manière très synthétique le mécanisme de sécurisation des ports, ou **Port Security**, qui peut (et devrait) être activé sur les commutateurs réseaux, dans le cas présent, ceux de la marque **CISCO**.


Systems and Network Analysis Center
Information Assurance Directorate

NATIONAL SECURITY AGENCY
Port Security on Cisco Access Switches

La première page est consacrée à la présentation des différents modes de traitement des adresses **MAC** (le niveau Ethernet) et des options de protection offertes. La seconde page détaille quelques exemples de configuration type.

Ce document, basic pour le spécialiste, a le mérite de présenter simplement et clairement ce que tout exploitant non versé dans la sécurité doit connaître des fonctions de sécurité de ce type d'équipement.

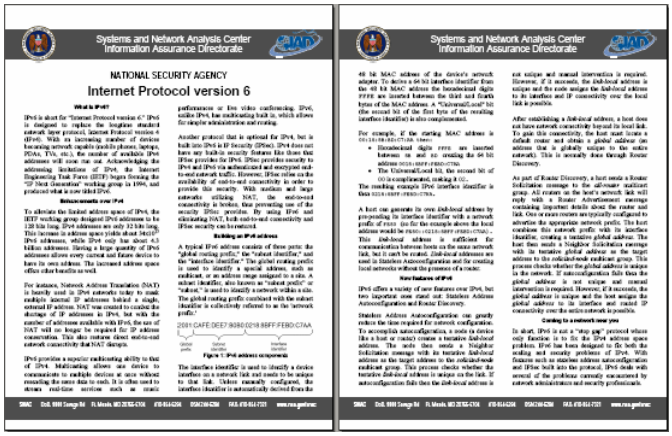
Un excellent document de vulgarisation qu'il conviendra de compléter par la lecture des manuels du constructeur dans le cas de la mise en œuvre de cette fonctionnalité sur les matériels d'autres fournisseurs.

- **Complément d'information**

http://www.nsa.gov/snac/switches/Factsheet-Cisco%20Port%20Security.pdf
http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.1E/native/configuration/guide/port_sec.html

NSA - INTERNET PROTOCOL VERSION 6

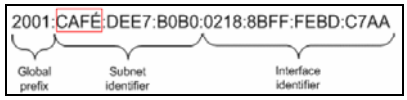
- **Description**



La **NSA** vient de publier un mémento de présentation du protocole Internet **IP V6**. Celui-ci est en cours de déploiement dans les infrastructures de la défense Américaine et au au cœur des réseaux des agences fédérales. Celles-ci devront avoir achevé cette migration au 30 juin 2008, aucune obligation ne leur étant faite d'étendre cette migration au-delà des réseaux fédérateurs.

Le plan de migration **IPv6** du **DoD**, établi en 2003, prévoyait son achèvement courant 2008 sans plus de précisions.

Le mémento de la **NSA** vient donc à point pour rafraîchir la mémoire des exploitants – et la notre par la même occasion - en nous rappelant les principes fondateurs du protocole IP version 6 dont l'intérêt principal - l'amélioration du niveau de sécurité n'étant qu'annexe - est de résoudre le délicat problème du trop faible espace d'adressage offert par la version 4 au regard des besoins actuels. L'appauvrissement en adresses disponibles est tel que certains experts s'accordent à dire qu'il n'y aura plus aucune adresse libre à l'horizon des années **2012** voire **2016**.



Si les équipements sont techniquement au point, il n'en va pas encore de même avec les hommes qui vont devoir apprendre à gérer la complexité de l'adressage. Il apparaît en effet illusoire de pouvoir mémoriser une adresse **IPv6** comme on pouvait le faire avec une adresse IPv4 quand bien même cette adresse contiendrait une séquence mnémotechnique comme celle présentée en exemple dans le mémento. Le lecteur se rassurera, les majuscules accentuées ne sont pas encore utilisées pour l'encodage hexadécimal des données.

- **Complément d'information**

http://www.nsa.gov/snac/voip/Factsheet-IPv6.pdf
http://www.cio-today.com/story.xhtml?story_id=57551 - Article sur les difficultés rencontrées par les agences

REFERENCES

CIS - CATALOGUE DE PROCEDURES ET DE TESTS

- **Description**

Le **CIS** – **Center for Internet Security** – vient d'annoncer la mise à jour du guide relatif aux environnements **Apache** et la publication d'un guide dédié à l'environnement **Microsoft Exchange Server 2007**. Aucun outil de validation associé n'est proposé.

P1 Profil N°1 – minimal, conservateur
P2 Profil N°2 – étendu, protectionniste
V Nouvelle version
M Mise à jour

Recommandations Systèmes			
Windows 2003 Domain controllers	P1	V2.0	Outil existant
Windows 2003 Member Servers	P1	V2.0	Outil existant
Windows XP Professional	P2	V2.01	Outil existant
Windows 2000 Professional	P2	V2.2.1	Outil existant
Windows 2000 Serveur	P2	V2.2.1	Outil existant
Windows 2000	P1	V1.2.2	Aucun outil prévu
Windows NT	P1	V1.0.5	Aucun outil prévu
Linux RedHat	P1	V1.0.5	Outil existant
Linux SuSE	P1	V1.0.0	Outil existant
Linux Slackware	P1	V1.1.0	Aucune planification
Linux Debian	P1	V1.0	Aucune planification
HP-UX	P1	V1.4.0	Outil existant
FreeBSD 4.8 et plus	P1	V1.0.5	Outil existant
Solaris 2.5.1 - 9	P1	V1.3.0	Outil existant
Solaris 10, 11/06 et 8/08	P1	V4.0	Outil existant
AIX 4.3.2, 4.3.3 et 5.1	P1	V1.0.1	Aucune planification
Mac OS/X 10.3 et sup.	P1	V2.0	Aucune planification
Novell OES:NetWare	P1	V1.0	Aucune information

Recommandations Equipements réseaux			
Wireless Networks	P1	V1.0	Aucun outil prévu
CISCO IOS routeurs	P1 P2	V2.2	Outil existant
CISCO PIX, ASA et FWSM	P1 P2	V2.2	Outil existant
CISCO CAR	*P1 P2*		
CheckPoint FW1/VPN1	P1 P2	V1.0	

Recommandations Applications				
M	**Apache WEB serveur toutes versions jusqu'à 2.2.6**	P1 P2	**V2.1**	Outil existant
	Oracle base de donnée 8i	P1 P2	V1.2	Outil existant
	Oracle base de donnée 9i et 10g	P1 P2	V2.0.1	Aucune planification
	Exchange Server 2003	P1	V1.0	Aucune planification
N	**Exchange Server 2007**	**P1**	**V1.0**	Aucune planification
	Microsoft SQL Serveur 2000	P2	V1.0	Aucune planification
	Microsoft SQL Serveur 2005	P1 P2	V1.0	Aucune planification
	MySQL 4.1, 5.0, et 5.1 Community Edition	P1 P2	V1.0	Aucune planification
	Bind Version 9	P1	V1.0	Aucune planification
	Novell eDirectory version 8.7	P1	V1.0	Aucune information
	Microsoft IIS Web Serveur	P1	V1.0	Aucune planification
	OpenLDAP	P1	V1.0	Aucune information
	FreeRadius	P1	V1.0	Aucune information
	Virtual Machines	P1	V1.0	Aucune information

Ces séries de tests sont déroulées à l'aide d'outils spécialisés pour la plate-forme cible à l'exception de la série de test des équipements réseaux **CISCO**.

Outils d'application				
Environnement Windows 2K/XP/2003	- ng_scoring_tool-gui-1.0-win32	exe	V1.0	WIN32
Environnement RedHat et SuSE	- ng_scoring_tool-1.0	tar	V1.0	LINUX+JAVA
Environnement FreeBSD	- cis_score_tool_freebsd_v1.7.2	tar	V1.7.2	FreeBSD
Environnement HP-UX	- cis_score_tool_hpux_v1.5.0	pkg	V1.5.0	HP-UX
Environnement Solaris 10	- cis_score_tool_solaris_v1.5.0	pkg	V1.5.0	SOLARIS
Environnement Solaris 2.5.1- 9	- CISscan	pkg		SOLARIS
Environnement CISCO	- CISRat	tar	V2.2	WIN32 UNIX
Environnement Oracle 8i	- CISscan	java		
Environnement Apache	- cis_score_tool_apache_v2.10	tar	V2.10	LINUX

- **Complément d'information**

http://www.cisecurity.org/ - Accès aux tests et outils associés
http://www.cisecurity.org/bench_exchange.html

DISA – GUIDES ET CHECKLISTS DE SECURISATION

- **Description**

La **DISA** a procédé à la mise à jour des listes de contrôle concernant les environnements **UNIX**, **Windows**, **OS/390** et **Desktop**.

[10 **M**ise(s) à jour, 0 **N**ouveau(x) document(s)]

		STIG			Checklist			
APPLICATIONS								
Applications	(Services)	1.1	17/01/06	PDF	2.1.10	01/12/07	PDF	
ESM		1.2	05/06/06	PDF				
ERP	(PeopleSoft, SAP)	1.1	10/04/07	PDF	1.0	01/06/06	DOC	
Database	(Générique + Oracle, SQL Server)	8.1	19/10/07	PDF	7.2.2	29/10/07	ZIP	
	(MS SQL Server 2005)				8.1.1	07/11/07	ZIP	
VoIP		2.2	21/04/06	PDF	2.2.2	19/05/06	PDF	
ENVIRONNEMENTS								
Access Control		2.1	17/10/07	PDF				
Directory Service		1.1	10/03/06	PDF	1.1.2	23/11/07	PDF	
Collaboration	(environnements collaboratifs)	1.1	28/03/07	ZIP	1.1	28/03/07	DOC	
Desktop		3.1	09/03/07	PDF	**3.1.3**	18/01/08	DOC	M
Enclave	(Périmètre)	4.1	21/06/07	PDF	4.1	21/06/07	PDF	
.NET	(Draft)				1.2	28/04/06	DOC	
Secure Remote Computing		1.2	10/08/05	DOC				
PERIPHERIQUES RESEAUX								
Sharing peripheral across the network		1.1	29/07/05	PDF				
- Multi-Function Device (MFD) and Printer Checklist					1.1.2	14/04/06	PDF	
- Keyboard, Video, and Mouse (KVM) Switch Checklist					1.1.2	14/04/06	PDF	
- Storage Area Network (SAN) Checklist					1.1.3	19/05/06	PDF	
- Universal Serial Bus (USB) Checklist					1.1.2	06/04/06	PDF	
RESEAU								
Network		7.1	25/10/07	PDF	7.1.1	21/11/07	PDF	
Cisco	(Supplément)				6.1	02/12/05	PDF	
Juniper	(Supplément)				6.4	02/12/05	PDF	
IP WAN					2.3	12/08/04	PDF	
Wireless	(Liste de contôle générique)	5.2.1	15/11/07	PDF	5.2.1	15/11/07	PDF	
Wireless	BlackBerry				5.2.1	15/11/07	PDF	
Wireless	Apriva				5.2.1	15/11/07	PDF	
Wireless	Motorola				5.2.1	15/11/07	PDF	
Wireless	Windows				5.2.1	15/11/07	PDF	

Wireless LAN Security Framework Addendum		2.1	31/10/05	PDF				
Wireless LAN Site Survey Addendum		1.1	31/10/05	PDF				
Wireless LAN Secure Remote Access Addendum		1.1	31/10/05	PDF				
Wireless Mobile Computing Addendum		1.1	31/10/05	PDF				
SERVICES								
DNS		4.1	17/10/07	PDF	3.1.1	10/04/07	PDF	
Web Servers	(Générique)	6.1	11/12/06	PDF	6.1.5	23/11/07	ZIP	
	(IIS)				6.1.5	23/11/07	ZIP	
	(iPlanet)				6.1.5	23/11/07	ZIP	
	(Apache)				6.1.5	23/11/07	ZIP	
	(TomCAT)				6.1.2	23/11/07	ZIP	
	(WebLogic)				6.1.2	23/11/07	ZIP	
SYSTEMES								
OS/390 & z/OS		5.2	19/09/06	PDF	**5.2.7**	17/01/08	DOC	M
OS/390 Logical Partition		2.2	04/03/05	PDF	2.1.4	04/06	DOC	
OS/390 RACF					**5.2.7**	17/01/08	DOC	M
OS/390 ACF2					**5.2.7**	17/01/08	DOC	M
OS/390 TSS					**5.2.7**	17/01/08	DOC	M
MacOS X		1.1	15/06/04	PDF	1.1.3	28/04/06	DOC	
TANDEM		2.2	04/03/05	PDF	2.1.2	17/04/06	DOC	
UNISYS		7.2	28/08/06	PDF	7.1.2	17/04/06	PDF	
UNIX		5.1	28/03/06	PDF	**5.1.10**	10/01/08	DOC	M
VM IBM		2.2	04/03/05	PDF	2.1.2	04/06	DOC	
SOLARIS	(2.6 à 2.9)				-	20/01/04	DOC	
VMS VAX					2.2.3	17/04/06	DOC	
Windows VISTA					**6.1.4**	10/01/08	ZIP	M
Windows 2003					**6.1.4**	10/01/08	ZIP	M
Windows 2000					**6.1.4**	10/01/08	ZIP	M
Windows XP		1.8	12/01/03	PDF	6.1.4	10/01/08	ZIP	M
Windows NT		3.1	26/12/02	DOC	4.1.21	28/07/06	DOC	
Windows 2000/XP/2003/Vista Addendum		6.1	21/05/07	PDF				
TECHNOLOGIES								
Biométrie		1.3	10/11/05	PDF	1.3.1	31/10/05	DOC	
SPECIFIQUE DoD								
Backbone transport		1.1	05/06/06	PDF	1.1.1	18/01/07	PDF	R
Defense switch network		2.3	30/04/06	PDF	2.3.2	01/05/06		R
Secure telecommunication Red switch network		1.1	26/03/06	PDF				R
DODI 8500.2 IA					1.1.1	18/01/07	PDF	R

N Nouveau M Mis à jour R Accès restreint

- **Complément d'information**

http://iase.disa.mil/stigs/index.html - Pages d'accueil
http://iase.disa.mil/stigs/stig/index.html - STIG
http://iase.disa.mil/stigs/checklist/index.html - Checklists

NSA - CATALOGUE DES GUIDES DE SECURITE

- **Description**

Deux mémentos techniques ont été publiés par la **NSA**. Ils sont intitulés '**Port Security on Cisco Access Switches**' et '**Internet Protocol Version 6**'.

G Guide de mise en œuvre et/ou manuel d'utilisation
R Recommandations et principes élémentaires
P Procédures et mise en application
N Document nouvellement publié
O Document obsolète

Windows VISTA

R	Windows Vista Security Guide	-	25/10/2006	MIC
I	How to Securely Configure Microsoft Windows Vista BitLocker		15/09/2007	NSA

Windows 2003

R	The Windows Server 2003 - Security Guide	V2.1	26/04/2006	MIC
R	NSA Windows Server 2003 Security Guide Addendum	V1.0	12/09/2006	NSA
R	Testing the Windows Server 2003 - Security Guide	V2.1	26/04/2006	MIC
R	Supporting the Windows Server 2003 - Security Guide	V2.1	26/04/2006	MIC
R	Delivering the Windows Server 2003 - Security Guide	V2.1	26/04/2006	MIC
G	Systems Management Server 2003 Security Guide	V1.0	01/04/2005	NSA
G	Exchange Server 2003 Benchmark	V1.0	-	CIS

Windows XP

Système

N	R	NSA Windows XP Security Guide Addendum	V1.0	12/09/2006	NSA

Windows 2000

Références					
	I	Microsoft Windows 2000 Network Architecture Guide	V1.0	19/04/2001	NSA
	I	Group Policy Reference	V1.08	02/03/2001	NSA
Systèmes					
	G	Guide to Securing Microsoft Windows 2000 Group Policy	V1.1	13/10/2001	NSA
	I	Guide to Securing Microsoft Windows 2000 Group Policy: Security Configuration Tool	V1.22	12/09/2006	NSA
	P	Guide to Securing Microsoft Windows 2000 File and Disk Resources	V1.01	26/11/2002	NSA
	P	Guide to Securing Microsoft Windows 2000 DNS	V1.0	09/04/2001	NSA
	P	Guide to Securing Microsoft Windows 2000 Encrypting File System	V1.0	01/01/2001	NSA
	P	Guide to Windows 2000 Kerberos Settings	V1.1	27/06/2001	NSA
	P	Microsoft Windows 2000 Router Configuration Guide	V1.02	01/05/2001	NSA
	R	Guide to Securing Windows NT/9x Clients in a Windows 2000 Network	V1.02	23/01/2001	NSA
Annuaire					
	I	Guide to Securing Microsoft Windows 2000 Schema	V1.0	06/03/2001	NSA
	I	Guide to Securing Microsoft Windows 2000 Active Directory	V1.0	01/12/2000	NSA
Certificats					
	R	Guide to the Secure Config. & Admin. of Microsoft Windows 2000 Certificate Services	V2.11	10/10/2001	NSA
	R	Guide to the Secure Config. & Admin. of Microsoft Windows 2000 Certificate Services (check)	V2.02	10/10/2001	NSA
	R	Guide to Using DoD PKI Certificates in Outlook 2000	V4.0	08/04/2002	NSA
Services annexes					
	I	Guide to Secure Configuration & Administration of Microsoft ISA Server 2000	V1.5	08/08/2002	NSA
	P	Guide to Securing Microsoft Windows 2000 DHCP	V1.3	19/07/2002	NSA
	P	Guide to Securing Microsoft Windows 2000 Terminal Services	V1.0	02/07/2001	NSA
	P	Microsoft Windows 2000 IPsec Guide	V1.0	13/08/2001	NSA
	P	Guide to the Secure Configuration and Administration of Microsoft Exchange 2000	V1.2	24/11/2003	NSA
Windows NT					
	P	Guide to Securing Microsoft Windows NT Networks	V4.2	18/09/2001	NSA
Unix					
	P	Guide to the Secure Configuration of Solaris 8	V1.0	09/09/2003	NSA
	P	Guide to the Secure Configuration of Solaris 9	V1.0	16/07/2004	NSA
	P	Apple Mac OS X v10.3.x Security configuration guide	V1.1	21/12/2004	NSA
	P	Apple Mac OS X Server v10.3.x Security configuration guide	V1.0	08/07/2005	NSA
	P	Apple Mac OS X v10.4.x Security configuration guide	Ed. 2	12/03/2007	Apple
	P	Apple Mac OS X Server v10.4.x Security configuration guide	Ed. 2	12/03/2007	Apple
	P	Guide to the Secure Configuration of Red Hat Enterprise Linux 5	-	19/11/2007	NSA
Cisco					
	R	Router Security Configuration Guide - Executive Summary	V1.1	03/03/2006	NSA
	P	Router Security Configuration Guide	V1.1c	15/12/2005	NSA
	P	Router Security Configuration Guide – Security for IPV6 Routers	V1.0	23/05/2006	NSA
	P	Cisco IOS Switch Security Configuration Guide	V1.0	21/06/2004	NSA
	I	Configuring a PC to Remotely Administer a Cisco Router Using the Router Console		18/05/2007	NSA
	I	Configuring a Cisco Router for Remote Administration Using the Router Console		04/05/2007	NSA
N	I	**Port Security on Cisco Access Switches**	-	08/01/2008	NSA
Sans-Fils					
	G	Guidelines for the Development and Evaluation of IEEE 802.11 IDS	V1.1	01/10/2005	NSA
	G	Recommended 802.11 Wireless Local Area Network Architecture	-	23/09/2005	NSA
	G	Security Guidance for Bluetooth Wireless Keyboards and Mice		26/09/2006	NSA
	I	So Your Boss Bought you a New Laptop How do you identify & disable wireless capabilities		04/06/2007	NSA
Contenus exécutables					
	O	Outlook E-mail Security in the Wake of Recent Malicious Code Incidents	V3.0	14/11/2003	NSA
	O	Guide to the Secure Configuration and Administration of Microsoft Exchange 5	V3.0	07/01/2002	NSA
	O	Microsoft Office 97 Executable Content Security Risks and Countermeasures	V1.1	20/12/1999	NSA
	R	Microsoft Office 2000 Executable Content Security Risks and Countermeasures	ND	08/02/2002	NSA
	R	Microsoft Office 2003 Executable Content Security Risks and Countermeasures	ND	05/02/2004	NSA
	I	Data Execution Prevention (DEP)		25/10/2007	NSA
Bases de données					
	R	Guide to the Secure Configuration and Administration of Microsoft SQL Server 2000	V1.5	15/01/2003	NSA
	R	Guide to the Secure Configuration and Administration of Oracle9i	V1.2	30/10/2003	NSA
	G	Oracle Application Server on Windows 2003 Security Guide	V1.2	12/2006	NSA
	G	Oracle Application Server Security Recommendations and DoDI 8500.2 IA Control		12/2006	NSA
	R	Benchmark for Oracle 9i/10g	V2.0	-	CIS
Web					
	R	BEA WebLogic Platform Security Guide	V1.0	04/04/2005	NSA
	P	Guide to the Secure Configuration & Administration of Microsoft IIS 5.0	V1.4	16/01/2004	NSA
	R	Guide to Securing Microsoft Internet Explorer 5.5 Using Group Policy	V1.0	07/2002	NSA
	R	Guide to Securing Netscape Navigator 7.02	V1.1	04/2003	NSA
Documents de Support					
	I	Defense in Depth	ND	ND	
	O	Guide to the Secure Configuration & Administration of iPlanet Web Serv Ent. Ed. 4.1	V1.73	03/07/2001	NSA
	O	Guide to the Secure Conf. and Admin. of Microsoft IIS 4.0	V1.33	04/03/2002	NSA
	O	Guide to the Secure Conf. and Admin. of Microsoft IIS 4.0 (Checklist Format)	V1.33	04/03/2002	NSA
	O	Secure Config. of the Apache Web Server, Apache Server V1.3.3 on Red Hat Linux 5.1	V1.12	24/04/2001	NSA

	R	Microsoft NetMeeting 3.0 Security Assessment and Configuration Guide	V1.14	05/10/2001	NSA
	R	The 60 Minute Network Security Guide	V2.1	15/03/2006	NSA
	R	Guide to Sun Microsystems Java Plug-in Security	V1.0	01/04/2004	NSA
	R	Guide to Microsoft .NET Framework Security	V1.5	11/11/2005	NSA
	I	Enterprise Firewall Types	-	01/08/2006	NSA
	I	Desktop or Enterprise Firewall ?	-	01/08/2006	NSA
	I	Enterprise Firewalls in Encrypted Environments	-	01/08/2006	NSA
	I	Security Guidance for Using Mail Clients		01/02/2007	NSA
	I	Mail Client Security Cheat Sheet		01/02/2007	NSA
	I	Secure Instant Messaging		01/02/2007	NSA
	I	Disabling USB Storage Drives		01/04/2007	NSA
	I	Biometrics Security Considerations			

VoIP

	R	Security Guidance for Deploying IP Telephony Systems		14/02/2006	NSA
	R	Recommended IP Telephony Architecture	V1.0	01/05/2006	NSA
N	P	**Internet Protocol Version 6**	-	08/01/2008	NSA

- **Complément d'information**

http://www.nsa.gov/snac/ - Portail d'accès aux guides
http://www.nsa.gov/snac/os/redhat/rhel5-guide-i731.pdf - Secure Configuration of Red Hat Enterprise Linux 5
http://www.nsa.gov/snac/os/redhat/rhel5-pamphlet-i731.pdf - Hardening tips
http://www.signal-spam.fr/index.php/frontend/blog/signal_spam_et_la_cnil_partenaires_dans_la_lutte_contre_le_spam

LOGICIELS LIBRES

LES SERVICES DE BASE

Les dernières versions des services de base sont rappelées dans les tableaux suivants. Nous conseillons d'assurer rapidement la mise à jour de ces versions, après qualification préalable sur une plate-forme dédiée.

RESEAU

Nom	Fonction	Ver.	Date	Source
BIND	Gestion de Nom (DNS)	9.4.2	21/11/07	http://www.isc.org/
DHCP	Serveur d'adresse	4.0.0	19/12/07	http://www.isc.org/
NTP4	Serveur de temps	4.2.4p4	10/09/07	http://ntp.isc.org/bin/view/Main/SoftwareDownloads
OpenNTPD	Serveur de temps	3.9	15/05/06	http://www.openntpd.org/

MESSAGERIE

Nom	Fonction	Ver.	Date	Source
IMAP4	Relevé courrier	2007	20/12/07	ftp://ftp.cac.washington.edu/imap/
POP3	Relevé courrier	4.0.9	21/03/06	ftp://ftp.qualcomm.com/eudora/servers/unix/popper/
POPA3D	Relevé courrier	1.0.2	23/05/06	http://www.openwall.com/popa3d/
SENDMAIL	Serveur de courrier	8.14.2	01/11/07	ftp://ftp.sendmail.org/pub/sendmail/

WEB

Nom	Fonction	Ver.	Date	Source
APACHE	Serveur WEB	1.3.41	19/01/08	http://httpd.apache.org/dist
		2.0.63	19/01/08	
		2.2.8	19/01/08	
ModSSL	API SSL Apache 1.3.39	2.8.30	12/09/07	http://www.modssl.org
MySQL	Base SQL	5.1.22	24/09/07	http://dev.mysql.com/doc/refman/5.1/en/news.html
		6.0.3	16/11/07	http://dev.mysql.com/doc/refman/6.0/en/news.html
SQUID	Cache WEB	2.6s18	29/11/07	http://www.squid-cache.org/Versions/
		3.0s1	10/01/08	

AUTRE

Nom	Fonction	Ver.	Date	Source
FreeRadius	Gestion de l'identité	2.0.1	22/01/08	http://www.freeradius.org/
INN	Gestion des news	2.4.3	22/03/06	http://www.isc.org/
OpenCA	Gestion de certificats	0.9.3	10/10/06	http://pki.openca.org/projects/openca/downloads.shtml
OpenLDAP	Gestion de l'annuaire	2.4.7	13/12/07	ftp://ftp.openldap.org/pub/OpenLDAP/openldap-release/
Samba	Gestion de fichiers	3.0.28	10/12/07	http://us1.samba.org/samba/
Tor	Anonymat	0.1.2.19	29/12/08	http://tor.eff.org/download.html

LES OUTILS

Une liste, non exhaustive, des produits et logiciels de sécurité du domaine public est proposée dans les tableaux suivants.

LANGAGES

Nom	Fonction	Ver.	Date	Source
Perl	Scripting	5.8.8	10/02/06	http://www.cpan.org/src/README.html
Python	Scripting	2.5.1	18/04/07	http://www.python.org/download/
Ruby	Scripting	1.8.6p111	23/12/07	http://www.ruby-lang.org/en/downloads/
PHP	WEB Dynamique	5.2.5	08/11/07	http://www.php.net/downloads.php

ANALYSE RESEAU

Nom	Fonction	Ver.	Date	Source
Dsniff	Boîte à outils	2.3	17/12/00	http://www.monkey.org/~dugsong/dsniff
EtterCap	Analyse & Modification	0.7.3	29/05/05	http://ettercap.sourceforge.net/index.php?s=history
Ethereal	Analyse multiprotocole	0.99.7	18/12/07	http://www.wireshark.org/ http://www.ethereal.com/
Nstreams	Générateur de règles	1.0.3	06/08/02	http://www.hsc.fr/ressources/outils/nstreams/download/
SamSpade	Boîte à outils	1.14	10/12/99	http://www.samspade.org/
TcpDump	Analyse multiprotocole	3.9.8	25/09/07	http://www.tcpdump.org/
Libpcap	Acquisition Trame	0.9.8	25/09/07	http://www.tcpdump.org/
TcpFlow	Collecte données	0.21	07/08/03	http://www.circlemud.org/~jelson/software/tcpflow/

WinPCap	Acquisition Trame	4.0.2	09/11/07	http://www.winpcap.org/news.htm

ANALYSE DE JOURNAUX

Nom	Fonction	Ver.	Date	Source
Analog	Journaux serveur http	6.00	19/12/04	http://www.analog.cx
AWStats	Analyse log	6.7	03/07/07	http://awstats.sourceforge.net/
fwLogWatch	Analyse log	1.1	17/04/06	http://cert.uni-stuttgart.de/projects/fwlogwatch/
OSSIM	Console de gestion	0.9.9rc5	08/08/07	http://www.ossim.net/
SnortSnarf	Analyse Snort	050314.1	05/03/05	http://www.snort.org/dl/contrib/data_analysis/snortsnarf/
WebAlizer	Journaux serveur http	2.01-10	24/04/02	http://www.mrunix.net/webalizer/download.html

ANALYSE DE SECURITE

Nom	Fonction	Ver.	Date	Source
BackTrack	Boîte à outils	3.0beta	14/12/07	http://www.remote-exploit.org/backtrack_download.html
curl	Analyse http et https	7.18.0	28/01/08	http://curl.haxx.se/
FIRE	Boîte à outils	0.4a	14/05/03	http://sourceforge.net/projects/biatchux/
Nessus	Vulnérabilité réseau	2.2.10	27/07/07	http://www.nessus.org/download/
		3.0.6	27/07/07	http://www.nessus.org/download/
Helix	Boîte à outils	1.9a	13/07/07	http://www.e-fense.com/helix/
Nikto	Analyse http et https	2.02	10/01/08	http://www.cirt.net/nikto/
nmap	Vulnérabilité réseau	4.53	17/01/08	http://www.insecure.org/nmap/nmap_changelog.html
Saint	Vulnérabilité réseau	6.7.2	28/01/08	http://www.saintcorporation.com/resources/updates.html
Sara	Vulnérabilité réseau	7.4.4	17/11/07	http://www-arc.com/sara/
Wikto	Analyse http et https	2.0.2924	03/01/08	http://www.sensepost.com/research/wikto/
Whisker	LibWhisker	2.4	03/07	http://www.wiretrip.net/rfp/lw.asp

CONFIDENTIALITE

Nom	Fonction	Ver.	Date	Source
GPG	Signature/Chiffrement	2.0.8	20/12/07	http://www.gnupg.org/news.en.html
GPG4Win	Signature/Chiffrement	1.0.6	29/08/06	http://www.gnupg.org/news.en.html
GPG S/MIME	Signature/Chiffrement	1.9.20	20/12/05	http://www.gnupg.org/news.en.html
LibGCrypt	Signature/Chiffrement	1.2.3	29/08/06	http://www.gnupg.org/news.en.html

CONTROLE D'ACCES RESEAU

Nom	Fonction	Ver.	Date	Source
Xinetd	Inetd amélioré	2.3.14	24/10/05	http://www.xinetd.org/

CONTROLE D'INTEGRITE

Nom	Fonction	Ver.	Date	Source
RootKit hunt	Compromission UNIX	1.3.0	27/09/07	http://www.rootkit.nl/projects/rootkit_hunter.html
ChkRootKit	Compromission UNIX	0.48	17/12/07	http://www.chkrootkit.org/
RKRevealer	Compromission WIN	1.71	01/11/06	http://www.microsoft.com/technet/sysinternals/default.mspx

DETECTION D'INTRUSION

Nom	Fonction	Ver.	Date	Source
P0f	Identification passive	2.0.8	06/09/06	http://lcamtuf.coredump.cx/p0f.shtml
Snort	IDS Réseau	2.8.0.1	28/11/07	http://www.snort.org/dl/

GENERATEURS DE TEST

Nom	Fonction	Ver.	Date	Source
NetDude &all	Rejeu de paquets	0.4.8a	24/06/07	http://netdude.sourceforge.net/download.html
Scapy	Génération de paquet	1.2.0.2	09/04/07	h http://hg.secdev.org/scapy/raw-file/tip/scapy.py

PARE-FEUX

Nom	Fonction	Ver.	Date	Source
IpFilter	Filtre datagramme	4.1.27	10/07	http://coombs.anu.edu.au/ipfilter/ip-filter.html
NetFilter	Pare-Feu IpTables	1.4.0	22/12/07	http://www.netfilter.org/projects/iptables/downloads.html

TUNNELS

Nom	Fonction	Ver.	Date	Source
OpenSSL	Pile SSL	0.9.8g	19/10/07	http://www.openssl.org/
OpenSSH	Pile SSH 1 et 2	4.7	04/09/07	http://www.openssh.com/
OpenSwan	Pile IPSec	2.4.9	17/07/07	http://www.openswan.org/code/
PuTTY	Terminal SSH2	0.60	30/04/07	http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html
Stunnel	Proxy https	4.21	28/10/07	http://www.stunnel.org
Zebedee	Tunnel TCP/UDP	2.4.1a	06/09/05	http://www.winton.org.uk/zebedee/

NORMES ET STANDARDS

LES PUBLICATIONS DE L'IETF

LES RFC

Du **27/12/2007** au **30/01/2008**, **26 RFC** ont été publiés dont 2 RFC ayant trait à la sécurité.

RFC TRAITANT DE LA SÉCURITÉ

Thème	Num	Date	Etat	Titre
TEL	5069	01/08	Inf	Security Threats and Requirements for Emergency Call Marking and Mapping
TLS	5077	01/08	Pst	Transport Layer Security (TLS) Session Resumption without Server-Side State

RFC TRAITANT DE DOMAINES CONNEXES A LA SECURITE

Thème	Num	Date	Etat	Titre
SIEVE	5235	01/08	Pst	Sieve Email Filtering: Spamtest and Virustest Extensions
SIP	5039	01/08	Inf	The Session Initiation Protocol (SIP) and Spam

AUTRES RFC

Thème	Num	Date	Etat	Titre
CRYPTO	5114	01/08	Inf	Additional Diffie-Hellman Groups for Use with IETF Standards
EPC	5134	01/08	Inf	A URN for the EPCglobal Electronic Product Code (EPC) and Related Standards
IETF	5012	01/08	Inf	Requirements for Emergency Context Resolution with Internet Technologies
	5111	01/08	Exp	Experiment in Exploratory Group Formation within the Internet Engineering Task Force (IETF)
ISIS	5089	01/08	Pst	IS-IS Protocol Extensions for Path Computation Element (PCE) Discovery
MIB	5060	01/08	Pst	Protocol Independent Multicast MIB
	5097	01/08	Pst	MIB for the UDP-Lite protocol
MOBILE	5142	01/08	Pst	Mobility Header Home Agent Switch Message
MPLS	5129	01/08	Pst	Explicit Congestion Marking in MPLS
NET	5113	01/08	Inf	Network Discovery and Selection Problem
OSPF	5088	01/08	Pst	OSPF Protocol Extensions for Path Computation Element (PCE) Discovery
PIM	5059	01/08	Pst	Bootstrap Router (BSR) Mechanism for Protocol Independent Multicast (PIM)
SIEVE	5228	01/08	Pst	Sieve: An Email Filtering Language
	5229	01/08	Pst	Sieve Email Filtering: Variables Extension
	5230	01/08	Pst	Sieve Email Filtering: Vacation Extension
	5231	01/08	Pst	Sieve Email Filtering: Relational Extension
	5232	01/08	Pst	Sieve Email Filtering: Imap4flags Extension
	5233	01/08	Pst	Sieve Email Filtering: Subaddress Extension
SIGCOMP	5112	01/08	Pst	The Presence-Specific Static Dictionary for Signaling Compression (Sigcomp)
SIP	5025	12/07	Pst	Presence Authorization Rules
TEL	5031	01/08	Pst	A Uniform Resource Name (URN) for Emergency and Other Well-Known Services
TRIP	5115	01/08	Pst	Telephony Routing over IP (TRIP) Attribute for Resource Priority

LES DRAFTS

Du **27/12/2007**au **30/01/2008**, 171 drafts ont été publiés : **132** drafts mis à jour, **39** nouveaux drafts, dont **7** drafts ayant directement trait à la sécurité.

NOUVEAUX DRAFTS TRAITANT DE LA SECURITE

Thème	Nom du Draft	Date	Titre
AAA	draft-ietf-mext-aaa-ha-goals-00	27/12	AAA Goals for Mobile IPv6
ADD	draft-hoffman-additional-key-words-00	15/01	Additional Key words to Indicate Requirement Levels
HTTP	draft-ietf-httpbis-security-properties-00	23/01	Security Requirements for HTTP
IPV6	draft-sdecugis-mext-kbit-issues-00	16/01	the Key Management Mobility Capability (K) flag in Mobile IPv6.
ISIS	draft-ietf-isis-rfc3567bis-00	17/01	IS-IS Cryptographic Authentication
SDP	draft-ietf-mmusic-sdp-dtls-00	23/01	SDP Indicators for Datagram Transport Layer Security (DTLS)
SIP	draft-york-spit-similarity-scenarios-00	16/01	SIP Usage Scenarios Similar to SPIT
	draft-fischer-sip-e2e-sec-media-00	23/01	End-to-End Security for DTLS-SRTP

MISE A JOUR DE DRAFTS TRAITANT DE LA SECURITE

Thème	Nom du Draft	Date	Titre
CMS	draft-ietf-smime-symkeydist-10	28/01	CMS Symmetric Key Management and Distribution
	draft-ietf-smime-sha2-02	28/01	Using SHA2 Algorithms with Cryptographic Message Syntax
DSKPP	draft-ietf-keyprov-dskpp-02	25/01	Dynamic Symmetric Key Provisioning Protocol (DSKPP)
GSS-API	draft-ietf-kitten-gssapi-domain-based-…-06	25/01	GSS-API Internationalization and Domain-Based Service Names
	draft-ietf-kitten-krb5-gssapi-…-names-05	25/01	GSS-API Domain-Based Service Names Mapping for Kerberos V

HTTP	draft-ietf-httpbis-p7-auth-01	13/01	HTTP/1.1, part 7: Authentication
IETF	draft-ietf-ipr-3978-incoming-06	18/01	Rights Contributors provide to the IETF Trust
IPSEC	draft-ietf-btns-connection-latching-05	10/01	IPsec Channels: Connection Latching
	draft-kato-ipsec-camellia-modes-06	21/01	Additional Modes of Operation for Camellia and Its Use With IPsec
	draft-sheffer-ipsec-secure-beacon-03	21/01	Secure Beacon: Securely Detecting a Trusted Network
OPENPGP	draft-ietf-openpgp-camellia-01	22/01	The Camellia Cipher in OpenPGP
OSPF	draft-ietf-ospf-hmac-sha-02	25/01	OSPF HMAC-SHA Cryptographic Authentication
PKIX	draft-ietf-pkix-ecc-subpubkeyinfo-02	25/01	Elliptic Curve Cryptography Subject Public Key Information
PKU2U	draft-zhu-pku2u-04	28/01	Public Key Cryptography Based User-to-User Authentication
RID	draft-moriarty-post-inch-rid-soap-02	28/12	IODEF/RID over SOAP
	draft-moriarty-post-inch-rid-02	27/12	Real-time Inter-network Defense
SATP	draft-gsenger-secure-anycast-...-protocol-01	23/01	secure anycast tunneling protocol (SATP)
SIP	draft-ietf-sip-media-security-requirements-02	22/01	Requirements of Media Security Management Protocols
SMIME	draft-ietf-smime-multisig-04	22/01	Multiple Signatures in S/MIME
TLS	draft-hajjeh-tls-identity-protection-03	28/01	Credential Protection Ciphersuites for Transport Layer Security
	draft-ietf-tls-rfc4346-bis-08	25/01	The Transport Layer Security (TLS) Protocol Version 1.2
	draft-ietf-tls-rsa-aes-gcm-01	13/01	RSA based AES-GCM Cipher Suites for TLS
	draft-ietf-tls-rfc4366-bis-01	14/01	Transport Layer Security (TLS) Extensions: Extension Definitions

DRAFTS TRAITANT DE DOMAINES CONNEXES A LA SECURITE

Thème	Nom du Draft	Date	Titre
BEHAVE	draft-ietf-behave-turn-06	22/01	Relay Extensions to Session Traversal Utilities for NAT (STUN)
BGP	draft-ietf-softwire-encaps-safi-00	24/01	BGP Encapsulation SAFI and BGP Tunnel Encapsulation Attribute
DIAMETER	draft-ietf-dime-diameter-api-05	16/01	The Diameter API
	draft-ietf-dime-rfc3588bis-10	22/01	Diameter Base Protocol
	draft-ietf-dime-diameter-qos-04	29/01	Diameter Quality of Service Application
	draft-ietf-dime-app-design-guide-06	23/01	Diameter Applications Design Guidelines
	draft-ietf-dime-qos-attributes-04	21/01	Quality of Service Attributes for Diameter
L2TP	draft-ietf-l2tpext-l2tp-ppp-07	13/01	PPP Tunneling Using Layer Two Tunneling Protocol Version 3
L3VPN	draft-ietf-l3vpn-2547bis-mcast-06	14/01	Multicast in MPLS/BGP IP VPNs
SYSLOG	draft-ietf-syslog-tc-mib-05	21/01	Textual Conventions for Syslog Management

AUTRES DRAFTS

Thème	Nom du Draft	Date	Titre
AVT	draft-rocky-avt-rtp-gsm-hr-00	24/01	Media Type Registration of GSM-HR payload Format
BCP84	draft-savola-bcp84-urpf-experiences-03	23/01	Experiences from Using Unicast RPF
BFD	draft-ietf-bfd-base-07	16/01	Bidirectional Forwarding Detection
	draft-ietf-bfd-multihop-06	16/01	BFD for Multihop Paths
	draft-ietf-bfd-v4v6-1hop-07	16/01	BFD for IPv4 and IPv6 (Single Hop)
	draft-ietf-bfd-generic-04	16/01	Generic Application of BFD
	draft-katz-ward-bfd-multipoint-01	16/01	BFD for Multipoint Networks
CALL	draft-worley-call-completion-01	29/01	Call Completion Implementation Details
DCON	draft-romano-dcon-xdsp-reqs-02	23/01	Requirements for the XCON-DCON Synchronization Protocol
	draft-romano-dcon-requirements-02	23/01	Requirements for Distributed Conferencing
	draft-romano-dcon-framework-02	23/01	A Framework for Distributed Conferencing
DHCP	draft-ietf-dhc-container-opt-00	24/01	Container Option for Server Configuration
DNS	draft-ietf-dnsext-axfr-clarify-06	22/01	DNS Zone Transfer Protocol (AXFR)
	draft-ietf-dnsext-rfc2672bis-dname-08	14/01	Update to DNAME Redirection in the DNS
	draft-ietf-dnsext-rfc2671bis-edns0-00	27/12	Revised extension mechanisms for DNS (EDNS0)
	draft-ietf-dnsext-dns-protocol-profile-01	20/01	The Modern DNS Implementation Guide
DTNRG	draft-irtf-dtnrg-ltp-09	20/01	Licklider Transmission Protocol - Specification
ESDS	draft-rezafard-esds-problem-statement-00	15/01	Extensible Supply-chain Discovery Service Problem Statement
EVALUAT	draft-xiao-evaluate-dml-01	22/01	An Evaluation Framework for Data Modeling Languages
FORCES	draft-ietf-forces-model-10	29/01	ForCES Forwarding Element Model
FTP	draft-rosenau-ftp-single-port-01	28/01	FTP EXTENSION ALLOWING IP FORWARDING (NATs)
GEOPRIV	draft-ietf-geopriv-http-location-delivery-04	14/01	HTTP Enabled Location Delivery (HELD)
HIP	draft-ahrenholz-hiprg-dht-02	14/01	HIP DHT Interface
HTTP	draft-ietf-httpbis-p1-messaging-01	13/01	HTTP/1.1, part 1: URIs, Connections, and Message Parsing
	draft-ietf-httpbis-p2-semantics-01	13/01	HTTP/1.1, part 2: Message Semantics
	draft-ietf-httpbis-p3-payload-01	13/01	HTTP/1.1, part 3: Message Payload and Content Negotiation
	draft-ietf-httpbis-p4-conditional-01	13/01	HTTP/1.1, part 4: Conditional Requests
	draft-ietf-httpbis-p5-range-01	13/01	HTTP/1.1, part 5: Range Requests and Partial Responses
	draft-ietf-httpbis-p6-cache-01	13/01	HTTP/1.1, part 6: Caching
IDNA	draft-alvestrand-idna-bidi-03	27/01	An updated IDNA criterion for right-to-left scripts
	draft-klensin-idnabis-issues-06	28/01	IDNA: Issues, Explanation, and Rationale
	draft-klensin-idnabis-protocol-03	28/01	Internationalizing Domain Names in Applications (IDNA): Protocol
IETF	draft-hoffman-tao4677bis-01	21/01	A Novice's Guide to the Internet Engineering Task Force
IMAP	draft-melnikov-imap-search-res-07	28/01	IMAP extension for referencing the last SEARCH result
	draft-melnikov-imapext-filters-03	28/01	IMAP4 extension for named searches (filters)
IPV4	draft-ietf-mip4-nemo-v4-base-08	22/01	Network Mobility (NEMO) Extensions for Mobile IPv4
IPV6	draft-ietf-mext-nemo-v4traversal-00	23/01	Mobile IPv6 support for dual stack Hosts and Routers (DSMIPv6)
	draft-ietf-mip6-hiopt-10	20/01	DHCP Option for Home Information Discovery in MIPv6
	draft-ietf-mipshop-fh80216e-06	30/01	Mobile IPv6 Fast Handovers over IEEE 802.16e Networks
	draft-vandevelde-v6ops-ra-guard-01	28/01	IPv6 RA-Guard

	draft-hain-ipv6-geo-addr-00	16/01	An IPv6 Geographic
	draft-shyam-hn-ipv6-00	23/01	Hierarchical Networking and IPv6
	draft-ietf-shim6-failure-detection-10	23/01	Failure Detection and Locator Pair Exploration Protocol for IPv6
	draft-ietf-v6ops-802-16-depl…-scenarios-07	28/01	IPv6 Deployment Scenarios in 802.16 Networks
	draft-ietf-v6ops-addr-select-ps-03	28/01	Problem Statement of Default Address Selection
	draft-ietf-v6ops-rfc3330-for-ipv6-04	15/01	Special-Use IPv6 Addresses
IRTF	draft-lim-irtf-sam-alm-api-00	21/01	ALM API for Topology Management and Network Layer …
IVIP	draft-whittle-ivip-arch-01	14/01	Ivip (Internet Vastly Improved Plumbing) Architecture
JFCM	draft-mltf-jfcm-cctags-00	22/01	multilingual/multiscript country code tags
KERB	draft-ietf-krb-wg-otp-preauth-02	17/01	OTP Preauthentication
L1VPN	draft-ietf-l1vpn-bgp-auto-discovery-03	21/01	BGP-based Auto-Discovery for L1VPNs
LDP	draft-delord-jounay-pwe3-ldp-aii-reach….-00	15/01	LDP extension for AII reachability
LEMONAD	draft-ietf-lemonade-architecture-01	29/12	LSupporting OMA Mobile Email (MEM) using Internet Mail
	draft-melnikov-lemonade-convert-disc….-00	24/01	Discovery of CONVERT parameters
LINK	draft-wbeebee-on-link-and-off-link-…-01	21/01	ND On-link and Off-link Determination
MAIL	draft-ietf-eai-scenarios-03	25/01	UTF-8 Mail: Scenarios
	draft-ietf-eai-dsn-06	21/01	Internationalized Delivery Status and Disposition Notifications
MANET	draft-chakeres-manet-manetid-02	18/01	MANET INSTANCE_ID TLV
MBONED	draft-guo-mboned-mfec-framework-01	27/12	Multicast Forwarding Equivalence Class [MFEC]
MEDIACT	draft-ietf-mediactrl-requirements-03	30/12	Media Server Control Protocol Requirements
	draft-ietf-mediactrl-vxml-01	16/01	SIP Interface to VoiceXML Media Services
MIB	draft-jinxiang-operations-and-m….ngi-00	31/12	Retriving MIB Information based on NGI
MIKEY	draft-ietf-msec-mikey-applicability-07	29/01	On the applicability of various MIKEY modes and extensions
MMUSIC	draft-ietf-mmusic-media-path-middleboxes-00	17/01	Analysis of Middlebox Interactions for Signaling Protocol
MONAMI6	draft-ietf-monami6-multiplecoa-05	27/01	Multiple Care-of Addresses Registration
MPLS	draft-ietf-ccamp-mpls-gmpls-interwork-…-05	13/01	Framework for MPLS-TE to GMPLS migration
	draft-ietf-ccamp-mpls-gmpls-interwork-…-04	13/01	Requirements to Support operation of MPLS-TE over GMPLS Net.
	draft-ietf-pce-inter-layer-frwk-06	21/01	Framework for PCE-Based Inter-Layer MPLS and GMPLS TE
	draft-ietf-pwe3-fc-encap-07	17/01	Encapsulation Methods for Transport of FC frames Over MPLS
NERD	draft-lear-lisp-nerd-03	23/01	NERD: A Not-so-novel EID to RLOC Database
NETCONF	draft-ietf-netconf-monitoring-00	15/01	NETCONF Monitoring Schema
	draft-linowski-netconf-dml-requirements-00	28/01	NETCONF Data Modeling Language Requirements
NFS	draft-ietf-nfsv4-minorversion1-19	29/01	NFS Version 4 Minor Version 1
	draft-ietf-nfsv4-minorversion1-dot-x-03	29/01	NFSv4 Minor Version 1 XDR Description
NSIS	draft-manner-nsis-user-guide-00	18/01	- A User's Guide to the NSIS Protocol Family
OSPF	draft-venkata-ospf-dynamic-hostname-02	29/01	Dynamic Hostname Exchange Mechanism for OSPF
P2POVER	draft-hardie-p2poverlay-pointers-00	27/01	Mechanisms for use in pointing to overlay networks, nodes, res…
PKIX	draft-ietf-pkix-rfc4055-update-00	23/01	Update for RSAES-OAEP Algorithm Parameters
RCDML	draft-presuhn-rcdml-00	28/01	Requirements for a Configuration Data Modeling Language
RFC2026	draft-carpenter-rfc2026-changes-02	16/01	Changes to the Internet Standards Process defined by RFC 2026
RFC2822	draft-resnick-2822upd-05	28/01	Internet Message Format
RMT	draft-ietf-rmt-bb-fec-ldpc-08	23/01	LDPC Staircase and Triangle FEC Schemes
	draft-ietf-rmt-pi-norm-revised-06	15/01	NACK-Oriented Reliable Multicast (NORM) Protocol
	draft-ietf-rmt-bb-norm-revised-03	28/01	Multicast Negative-Acknowledgment (NACK) Building Blocks
ROHC	draft-sandlund-rohc-rfc4995bis-00	11/01	The RObust Header Compression (ROHC) Framework
	draft-ietf-rohc-rfc3095bis-rohcv2-profiles-05	29/01	ROHCv2: Profiles for RTP, UDP, IP, ESP and UDP Lite
RPC	draft-rosenau-rpc-dynnames-00	28/01	DYNAMIC RPC NUMBER ASSIGNMENT AND DISTRIBUTION
RSERPOO	draft-ietf-rserpool-mib-05	10/01	Management Information Base using SMIv2
	draft-ietf-rserpool-overview-03	22/01	An Overview of Reliable Server Pooling Protocols
RTP	draft-ietf-avt-rtp-atrac-family-13	23/01	RTP Payload Format for Adaptive TRansform Acoustic Coding
	draft-ietf-avt-rtp-hdrext-14	10/01	A general mechanism for RTP Header Extensions
	draft-ietf-avt-rtp-svc-06	21/01	RTP Payload Format for SVC Video
	draft-ietf-avt-rtp-uemclip-03	24/01	RTP payload format for mU-law UEMCLIP speech codec
	draft-ietf-avt-rtp-h264-rcdo-00	27/12	RTP Payload Format for H.264 RCDO Video
	draft-sollaud-avt-rfc4749-dtx-update-00	21/01	G.729.1 RTP Payload Format update: DTX support
SDP	draft-ietf-mmusic-connectivity-precon-04	23/01	Connectivity Preconditions for SDP Media Streams
	draft-ietf-mmusic-qos-identification-01	24/01	Quality of Service (QoS) Mechanism Selection in SDP
	draft-dondeti-oma-mmusic-sdp-attrs-00	31/12	SDP Attributes for OMA BCAST Service and Content Protection
SIEVE	draft-ietf-sieve-notify-xmpp-08	30/12	Sieve Notification Mechanism: xmpp
SIG	draft-housley-internet-draft-sig-file-01	24/01	Digital Signatures on Internet-Draft Documents
SIMPLE	draft-ietf-simple-partial-notify-10	21/01	SIP extension for Partial Notification of Presence Information
	draft-ietf-simple-imdn-06	14/01	Instant Message Disposition Notification
	draft-ietf-simple-chat-01	28/01	Multi-party Instant Message (IM) Sessions Using the MSRP
SIP	draft-johnston-sipping-cc-uui-03	15/01	Transporting User to User Call Control Information in SIP for ISDN
	draft-rosenberg-sip-ua-loose-route-02	25/01	Applying Loose Routing to (SIP User Agents (UA)
	draft-worley-service-example-01	16/01	Session Initiation Protocol Service Example -- Music on Hold
	draft-holmberg-sip-target-uri-delivery-01	16/01	Target URI delivery in the Session Initiation Protocol (SIP)
	draft-loreto-simple-im-srv-label-00	23/01	IANA Registration of Instant Messaging SRV Protocol Label
	draft-saito-sip-rendezvous-00	29/01	Analysis of Rendezvous Mechanism for Home Access Using SIP
	draft-ietf-sip-body-handling-01	23/01	Message Body Handling in the Session Initiation Protocol (SIP)
	draft-ietf-sipping-overload-reqs-02	25/01	Requirements for Management of Overload in SIP
	draft-ietf-sipping-sip-offeranswer-05	16/01	SIP (Session Initiation Protocol) Usage of the Offer/Answer Model
SMTP	draft-ietf-eai-smtpext-11	27/01	SMTP extension for internationalized email address
	draft-hansen-4468upd-mailesc-registry-03	10/01	A Registry for SMTP Enhanced Mail System Status Codes
SNMP	draft-schoenw-nmrg-snmp-trace-defi…-00	15/01	SNMP Trace Analysis Definitions
	draft-ietf-opsawg-snmp-engineid-disc…01	21/01	SNMP Context EngineID Discovery
SOFTWIR	draft-ietf-softwire-hs-framework-l2tpv2-08	29/01	Softwire Hub & Spoke Deployment Framework with L2TPv2

	draft-ietf-softwire-mesh-framework-03	14/01	Softwire Mesh Framework
	draft-ietf-softwire-bgp-te-attribute-00	23/01	Traffic Engineering Attribute
SPEERMI	draft-ietf-speermint-terminology-15	29/01	SPEERMINT Terminology
TCP	draft-ietf-dccp-rfc3448bis-04	25/01	TCP Friendly Rate Control (TFRC): Protocol Specification
	draft-briscoe-tsvwg-re-ecn-tcp-05	10/01	Re-ECN: Adding Accountability for Causing Congestion to TCP/IP
	draft-ietf-tcpm-1323bis-00	29/01	TCP Extensions for High Performance
TEXT	draft-hellstrom-textpreview-05	29/01	Presentation of Text Conversation in realtime and en-bloc form
	draft-hellstrom-text-turntaking-01	10/01	Registration of the Real-time-text Media Feature Tag
TSVWG	draft-floyd-tsvwg-besteffort-03	29/01	Comments on the Usefulness of Simple Best-Effort Traffic
VCARD	draft-resnick-vcarddav-vcardrev-00	18/01	vCard Format Specification
VDSL	draft-ietf-adslmib-vdsl2-04	29/01	Definitions of Managed Objects for VDSL2
WEBDAV	draft-godoy-webdav-xmlsearch-01	25/01	A WebDAV Search Grammar for XML Properties
XMPP	draft-saintandre-xmpp-presence-analysis-03	16/01	Interdomain Presence Scaling Analysis for XMPP

NOS COMMENTAIRES

LES DRAFTS

DRAFT-IETF-SIPPING-SBC-FUNCS-04

Requirements from SIP Session Border Control Deployments

Elaboré par le groupe de travail '**SIPPING**' - **S**ession **I**nitiation **P**roposal **IN**vesti**G**ation - et résultant de la collaboration de plusieurs experts travaillant pour des sociétés spécialisées dans la téléphonie avec la société **Ericsson** ou dans les services associés avec les sociétés **3CLogic** ou encore **Ditech Network Inc.**, ce document intéressera aussi bien les spécialistes du protocole **SIP** que ceux de la sécurité.

Il propose en effet une synthèse des fonctionnalités actuellement offertes par les équipements de médiation et de contrôle dénommés '**SBC**' ou '**Session Border Controller**' généralement positionnés à la frontière du réseau d'entreprise. Il s'intéresse plus particulièrement aux fonctions et procédés mis en œuvre dans ces équipements susceptibles d'impacter le bon fonctionnement ou la qualité de service car entrant en conflit avec les spécifications initiales du protocole **SIP**, et de lui seul.

On notera que, pour être à même d'intervenir sur les flux échangés entre entités homologues, ces équipements devront bien souvent se positionner en tant qu'intermédiaires se faisant passer pour l'entité tierce, une approche bien connue dans le monde de la sécurité et désignée par deux termes: '**proxy**' lorsque la fonction a pour objectif de renforcer la sécurité aux interfaces d'un réseau, '**Man-in-the-Middle**' ou '**MiTM**' lorsqu'elle est employée par un tiers malveillant dans le but d'intercepter un échange de données normalement sécurisé. Ce dernier terme est d'ailleurs explicitement mentionné au paragraphe '3.7.2 – Media Encryption – Architectural Issues' qui détaille le fonctionnement d'un '**SBC**' en tant que médiateur chargé d'assurer le déchiffrement d'une communication – sans que l'usager n'en soit averti - avant transport de celle-ci sur le réseau d'un opérateur.

Le chapitre, mandataire, '**Security Considerations**' rappelle que la majorité des fonctionnalités discutées dans le document ont un rapport direct avec la sécurité, le positionnement des '**SBC**' en faisant par ailleurs d'excellentes cibles pour des attaques en déni de service.

Un court chapitre est consacré aux améliorations qui devraient/pourraient être apportées à une prochaine version du protocole **SIP** afin de résoudre certaines problématiques exposées. Trois propositions d'évolution sont ici énumérées:

1- Offrir un moyen 'propre' permettant de masquer la topologie du réseau interne sans avoir à devoir recourir à la manipulation et au remplacement de certains en-têtes positionnés par les entités demandant à être mise en relation,

2- Offrir un moyen 'propre' permettant de rediriger les flux sur des points de relayage intermédiaires sans avoir à devoir manipuler, sans le consentement de l'usager, les descripteurs de session. Cette fonctionnalité est requise pour répondre aux exigences législatives de très nombreux pays en matière d'interception légale,

3- Disposer d'un mécanisme permettant de gérer les discordances ou incohérences dans les en-têtes des messages dues à des choix d'implémentation qui divergent. Les cas de l'implémentation **SIP** des plateformes **3GPP** et du ré-adressage **IPv4**/**IPv6** sont cités.

La table des matières de ce document de 24 pages est la suivante:

http://www.ietf.org/internet-drafts/draft-ietf-sipping-sbc-funcs-04.txt

ALERTES ET ATTAQUES

ALERTES

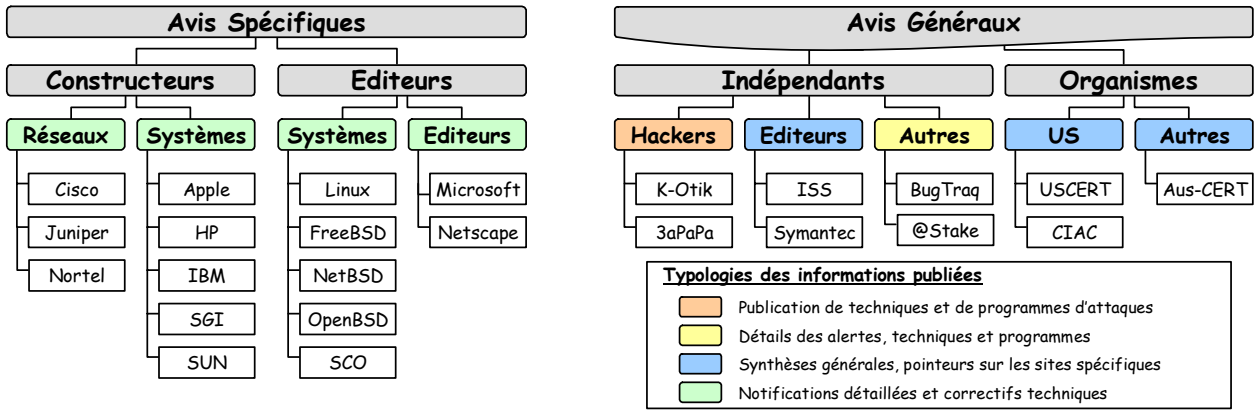
GUIDE DE LECTURE

La lecture des avis publiés par les différents organismes de surveillance ou par les constructeurs n'est pas toujours aisée. En effet, les informations publiées peuvent être non seulement redondantes mais aussi transmises avec un retard conséquent par certains organismes. Dès lors, deux alternatives de mise en forme de ces informations peuvent être envisagées :

- o Publier une synthèse des avis transmis durant la période de veille, en classant ceux-ci en fonction de l'origine de l'avis,
- o Publier une synthèse des avis transmis en classant ceux-ci en fonction des cibles.

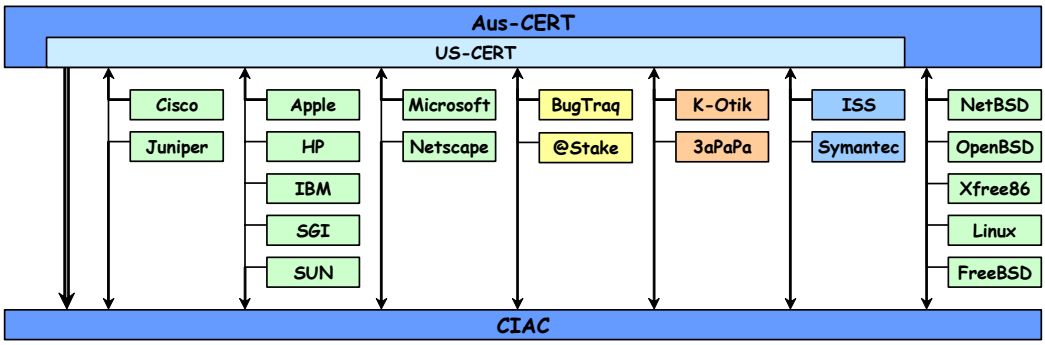
La seconde alternative, pour séduisante quelle soit, ne peut être raisonnablement mise en œuvre étant donné l'actuelle diversité des systèmes impactés. En conséquence, nous nous proposons de maintenir une synthèse des avis classée par organisme émetteur de l'avis.

Afin de faciliter la lecture de ceux-ci, nous proposons un guide de lecture sous la forme d'un synoptique résumant les caractéristiques de chacune des sources d'information ainsi que les relations existant entre ces sources. Seules les organismes, constructeurs ou éditeurs, disposant d'un service de notification officiel et publiquement accessible sont représentés.



L'analyse des avis peut être ainsi menée selon les trois stratégies suivantes :

- o Recherche d'informations générales et de tendances : Lecture des avis du CERT et du CIAC
- o Maintenance des systèmes : Lecture des avis constructeurs associés
- o Compréhension et anticipation des menaces : Lecture des avis des groupes indépendants



FORMAT DE LA PRESENTATION

Les alertes et informations sont présentées classées par sources puis par niveau de gravité sous la forme de tableaux récapitulatifs constitués comme suit :

Présentation des Alertes

EDITEUR			
TITRE			
Description sommaire			
Gravité	Date	Informations concernant la plate-forme impactée	
Correction		Produit visé par la vulnérabilité	Description rapide de la source du problème
Référence		URL pointant sur la source la plus pertinente	
Référence(s) CVE si définie(s)			

Présentation des Informations

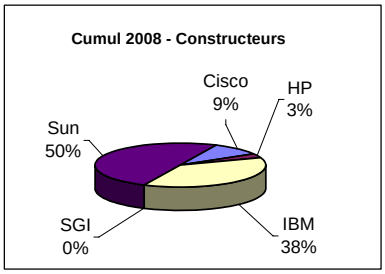
SOURCE
TITRE
Description sommaire
URL pointant sur la source d'information
Référence(s) CVE si définie(s)

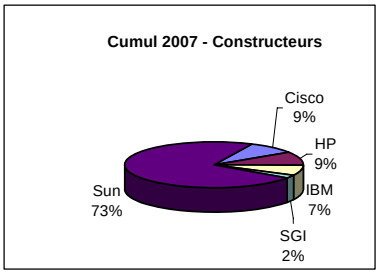
SYNTHESE MENSUELLE

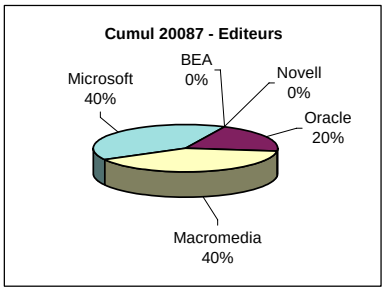
Le tableau suivant propose un récapitulatif du nombre d'avis publiés pour la période courante, l'année en cours et l'année précédente. Ces informations sont mises à jour à la fin de chaque période de veille. L'attention du lecteur est attirée sur le fait que certains avis sont repris et rediffusés par les différents organismes. Ces chiffres ne sont donc représentatifs qu'en terme de tendance et d'évolution.

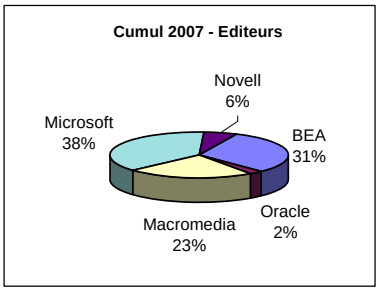
Période du **27/12/2007** au **30/01/2008**

		Cumul	
	Période	2008	2007
Organisme	**27**	**27**	**324**
US-CERT TA	3	3	39
US-CERT ST	2	2	23
CIAC	22	22	262
Constructeurs	**32**	**32**	**482**
Cisco	3	3	43
HP	1	1	45
IBM	12	12	35
SGI	0	0	11
Sun	16	16	348
Editeurs	**5**	**5**	**165**
BEA	0	0	51
Oracle	1	1	4
Macromedia	2	2	38
Microsoft	2	2	62
Novell	0	0	10
Unix libres	**157**	**157**	**1 164**
Linux RedHat	19	19	257
Linux Fedora	59	59	409
Linux Debian	42	42	175
Linux Mandr.	28	28	232
Linux SuSE	7	7	82
FreeBSD	2	2	9
Autres	**13**	**13**	**215**
iDefense	13	13	173
eEye	0	0	11
NGS Soft.	0	0	31









ALERTES DETAILLEES

AVIS OFFICIELS

Les tables suivantes présentent une synthèse des principales alertes de sécurité émises par un organisme fiable, par l'éditeur du produit ou par le constructeur de l'équipement. Ces informations peuvent être considérées comme fiables et authentifiées. En conséquence, les correctifs proposés, s'il y en a, doivent immédiatement être appliqués.

APACHE

Exécution de code 'SQL' arbitraire dans 'Derby'			
Un manque de validation dans 'Derby' d'Apache permet à un attaquant d'exécuter du code 'SQL' arbitraire.			
Moyenne	28/01	Apache ' Derby' versions inférieures à 10.2.1.6	
Correctif existant	'DropSchemaNode'	Manque de validation	
Apache	http://issues.apache.org/jira/browse/DERBY-1858		
CVE-2006-7217			

Multiples failles via le module 'mod_proxy_balancer'			
Deux failles permettent de provoquer un déni de service et des attaques de type "Cross-Site Scripting".			
Forte	10/01	Apache 'Apache' versions 2.2.0 à 2.2.6	
Correctif existant	Module 'mod_proxy_balancer'	Non disponible	
Apache	http://httpd.apache.org/security/vulnerabilities_22.html		
CVE-2007-6421, CVE-2007-6422			

ASTERISK

Déni de service via le pilote 'SIP channel'			
Une erreur de codage permet à un attaquant distant de provoquer un déni de service d'un produit vulnérable.			
Forte	02/01	Se référer à l'avis original	
Correctif existant	Pilote 'SIP channel'	Erreur de codage	
Asterisk	http://downloads.digium.com/pub/security/AST-2008-001.html		

CISCO

Accès non autorisé dans Cisco 'AVS'			
Une erreur de conceptionpermet à un attaquant distant d'obtenir un accès non autorisé au produit.			
Forte	23/01	Cisco 'Application Velocity System' versions inférieures à 5.1.0	
Correctif existant	Mot de passe par défaut	Erreur de conception	
Cisco	http://www.cisco.com/warp/public/707/cisco-sa-20080123-avs.shtml		
CVE-2008-0029			

Déni de service dans 'CallManager' (CUCM)			
Un débordement de buffer permet à un attaquant d'exécuter du code arbitraire et de provoquer un déni de service.			
Critique	17/01	Se référer à l'avis original	
Correctif existant	Port TCP/2444	Débordement de buffer	
Cisco	http://www.cisco.com/warp/public/707/cisco-sa-20080116-cucmctl.shtml		
CVE-2008-0027			

Déni de service dans Cisco 'PIX' et 'ASA'			
Une faille permet de provoquer un déni de service de ces équipements.			
Forte	23/01	Se référer à l'avis original	
Correctif existant	Fonctionnalité 'TTL decrement'	Non disponible	
Cisco	http://www.cisco.com/warp/public/707/cisco-sa-20080123-asa.shtml		
CVE-2008-0028			

CORE SECURITY TECH.

Elévation de privilèges dans 'CORE FORCE'			
Un débordement de buffer autorise un utilisateur à provoquer un déni de service ou à obtenir des droits privilégiés.			
Moyenne	17/01	Core Security Technologies 'CORE FORCE' version 0.95.167 et inférieures	
Correctif existant	Non disponible	Débordement de buffer	
Core Security T.	http://www.coresecurity.com/?action=item&id=2025		

DOVECOT

Elévation de privilèges dans 'Dovecot'			
Une erreur de conception permet à un utilisateur d'obtenir les droits d'un autre utilisateur.			
Moyenne	21/12	Dovecot 'Dovecot' versions 1.0.8 et 1.0.9	
Correctif existant	Authentification 'LDAP'	Erreur de conception	
Dovecot	http://www.dovecot.org/list/dovecot-news/2007-December/000057.html		

DRUPAL

"Cross-Site Scripting" dans 'Drupal'

Un manque de validationpermet à un attaquant de mener des attaques de type "Cross-Site Request Forgery".

Forte	14/01	Drupal 'BUEditor' version 4.7.x-1.0 et inférieures, versions inférieures à 5.x-1.1	
Correctif existant		Requêtes 'HTTP'	Manque de validation
Drupal		http://drupal.org/node/208534	

"Cross-Site Scripting" dans Drupal ('Archive')

Un manque de validation permet à un attaquant de mener des attaques de type "Cross-Site Scripting".

Forte	25/01	Drupal 'Archive' version 5.x	
Correctif existant		Paramètres non spécifiés	Manque de validation
Drupal		http://drupal.org/node/213478	

"Cross-Site Scripting" dans Drupal ('Workflow')

Un manque de validation permet à un attaquant de mener des attaques de type '"Cross-Site Scripting".

Forte	25/01	Drupal 'Workflow' version 4.7.x et version 5.x	
Correctif existant		Messages 'workflow'	Manque de validation
Drupal		http://drupal.org/node/213473	

Exécution de code arbitraire dans 'Meta Tags'

Une erreur de traitement dans le produit Drupal permet à un attaquant distant d'exécuter du code arbitraire.

Forte	15/01	Drupal 'Meta Tags' version 5.x-1.6	
Correctif existant		Module 'Meta tags' (Nodewords)	Erreur de traitement des noeuds
Drupal		http://drupal.org/node/209759	

Multiples failles dans 'drupal'

De multiples failles permettent des attaques de types "Cross-Site Request Forgery" et "Cross-Site Scripting".

Forte	10/01	Drupal 'Drupal' versions inférieures à 4.7.11et inférieures à 5.6	
Correctif existant		Module 'aggregator'	Erreur de codage et de configuration
Drupal		http://drupal.org/node/208562 http://drupal.org/node/208565 http://drupal.org/node/208564	

HP

Déni de service dans 'HP-UX'

Une faille non documentée permet à un attaquant distant de provoquer un déni de service.

Forte	24/01	HP 'HP-UX ' version B.11.31	
Correctif existant		Non disponible	Non disponible
HP		http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01328657	
CVE-2007-6425			

IBM

Exécution de code dans Tivoli Storage Manager Express

Un débordement de tas permet d'exécuter du code arbitraire avec des droits privilégiés.

Forte	11/01	IBM 'Tivoli Storage Manager Express' versions inférieures à 5.3.7.3	
Correctif existant		Non disponible	Débordement de tas
IBM		http://www-1.ibm.com/support/docview.wss?uid=swg21291536	

Multiples vulnérabilités dans 'Informix Dynamic Server'

De multiples problèmes affectent le serveur de base de données IDS ('Informix Dynamic Server').

Forte	17/01	IBM 'Informix Dynamic Server' versions inférieures à 10.00.xC8	
Correctif existant		Multiples	Traversée de répertoires, création non sécurisée de fichiers
IBM		http://www-1.ibm.com/support/docview.wss?uid=swg27011556	

Déni de service dans un produit IBM Tivoli

Une faille permet de provoquer un déni de service de celui-ci.

Forte	22/01	IBM 'Tivoli Provisioning Manager for OS Deployment' version 5.1.0.3	
Correctif existant		Serveur 'HTTP'	Non disponible
IBM		http://www-1.ibm.com/support/docview.wss?uid=swg24018010	

Multiples failles dans 'Informix Dynamic Server'

Des débordements permettent de provoquer l'exécution de code arbitraire.

Forte	30/01	IBM 'Informix Dynamic Server' version 10.00.x et inférieures et version 11.10.x et inférieures	
Correctif existant		Bibliothèque 'XDR'	Débordement de pile, débordement de tas
IBM		http://www-1.ibm.com/support/docview.wss?uid=swg21294211	

Vulnérabilité dans 'WebSphere Business Modeler'			
Une faille permet à un utilisateur non privilégié de supprimer des fichiers qui ne lui appartiennent pas.			
Moyenne	23/01	IBM 'WebSphere Business Modeler Advanced' et 'Basic' version 6.0.2.1	
Correctif existant		Gestion des droits utilisateurs	Erreur de conception
IBM		http://www-1.ibm.com/support/docview.wss?uid=swg24018060	
IBM		http://www-1.ibm.com/support/docview.wss?uid=swg24018061	

Faille dans Tivoli 'Business Service Manager'			
Deux failles dans le produit IBM 'Tivoli Business Service Manager' provoquent l'exposition d'informations sensibles.			
Moyenne	22/01	IBM 'Tivoli Business Service Manager' version 4.1.1	
Correctif existant		'SM_server.log' et 'reconfig'	Erreur de conception
IBM		http://www-1.ibm.com/support/docview.wss?uid=swg24017939	

Déni de service dans 'Lotus Domino'			
Une faille non documentée dans 'Lotus Domino' permet de provoquer un déni de service.			
N/A	10/01	IBM 'Lotus Domino' versions inférieures à 7.0.2 Fix Pack 3	
Correctif existant		Non disponible	Non disponible
IBM		http://www-1.ibm.com/support/docview.wss?uid=swg27011539	

Déni de service via IBM 'HMC'			
Une faille permet de provoquer un déni de service d'un composant.			
N/A	30/01	IBM 'Hardware Management Console' version 7R3.2.0	
Correctif existant		'Pegasus CIM Server'	Non disponible
IBM		https://www14.software.ibm.com/webapp/set2/sas/f/hmc/power6/install/v7.Readme.html	

Vulnérabilité dans IBM 'AIX'			
Une faille non documentée et aux conséquences inconnues affecte la plate-forme 'AIX' d'IBM.			
N/A	08/01	IBM 'AIX' version 6.1	
Correctif existant		'trustchk_block_write()'	Non disponible
IBM		http://www-1.ibm.com/support/docview.wss?uid=isg1IZ12119	

Vulnérabilités dans 'WebSphere Application Server'			
Deux failles non documentées, et aux conséquences inconnues, affectent le produit 'WebSphere Application Server'.			
N/A	23/01	IBM 'WebSphere Application Server' versions inférieures à 6.0.2.25	
Correctif existant		Se référer à l'avis original	Non disponible
IBM		http://www-1.ibm.com/support/docview.wss?uid=swg27006876	
IBM		http://www-1.ibm.com/support/docview.wss?uid=swg27006876	

ICU

Exécution de code via la bibliothèque 'ICU'			
Deux failles permettent l'exécution de code arbitraire dans les applications l'utilisant.			
Moyenne	22/01	ICU 'ICU' version 3.8 et inférieures	
Correctif existant		Expressions régulières	Erreur de conception
Red Hat		http://rhn.redhat.com/errata/RHSA-2008-0090.html	

INGATE

Déni de service dans les produits Ingate			
Une faille dans le module 'SIP' des produits Ingate 'Firewall' et 'SIParator' permet de provoquer un déni de service.			
Forte	10/01	Ingate 'Firewall' versions inférieures à 4.6.1 et 'SIParator' versions inférieures à 4.6.1	
Correctif existant		Module 'SIP'	Erreur de conception
Ingate		http://www.ingate.com/relnote-461.php	

JETTY

Exposition d'informations dans le serveur 'Jetty'			
Une erreur de codage permet à un attaquant distant d'obtenir des informations sensibles.			
Forte	03/01	JETTY 'Jetty' version 6.1.5 et version 6.1.6	
Correctif existant		URLs contenants '//'	Erreur de codage
US-CERT		http://www.kb.cert.org/vuls/id/553235	

LINUX

Déni de service dans le noyau Linux			
Un débordement de buffer permet à un utilisateur local de provoquer un déni de service d'une plate-forme.			
Forte	30/01	Linux 'Noyau 2.6' version 2.6.23	
Correctif existant		Fichier 'isdn_common.c'	Débordement de buffer
Debian		http://www.debian.org/security/2008/dsa-1479	
CVE-2007-6151			

MANTIS

"Cross-Site Scripting" dans l'application 'Mantis'

Un manque de validationpermet à un attaquant de mener des attaques de type "Cross-Site Scripting".

Forte	22/01	Mantis 'Mantis' versions inférieures à 1.1.1	
Correctif existant		Page 'Summary'	Validation insuffisante des données en entrée
Mantis		http://sourceforge.net/project/shownotes.php?release_id=569765	

MICROSOFT

Exécution de code via la pile 'TCP/IP' de Windows

Deux failles dans la pile 'TCP/IP' permettent de provoquer des dénis de service et l'exécution de code arbitraire.

Critique	08/01	Se référer à l'avis original	
Correctif existant		Pile 'TCP/IP'	Non disponible
Microsoft		http://www.microsoft.com/technet/security/Bulletin/MS08-001.mspx	
CVE-2007-0066, CVE-2007-0069			

Elévation de privilèges via 'LSASS'

Une faille permet à un utilisateur local d'obtenir des droits privilégiés.

Forte	08/01	Se référer à l'avis original	
Correctif existant		Processus 'LSASS'	Erreur de conception
Microsoft		http://www.microsoft.com/technet/security/Bulletin/MS08-002.mspx	
CVE-2007-5352			

OPENAFS

Déni de service dans 'OpenAFS'

Une faille dans 'OpenAFS' permet de provoquer un déni de service d'un serveur vulnérable.

Forte	20/12	OPENAFS 'OpenAFS' versions 1.3.50 à 1.4.5 et versions 1.5.0 à 1.5.27	
Correctif existant		Gestionnaire RPC	Conflit d'accès aux ressources
OpenAFS		http://www.openafs.org/security/OPENAFS-SA-2007-003.txt	
CVE-2007-6599			

ORACLE

Nombreuses failles dans les produits Oracle

De multiples vulnérabilités dans les produits Oracle peuvent entraîner de nombreuses conséquences.

Critique	16/01	Se référer à l'avis original	
Correctif existant		Se référer à l'avis original	Multiples vulnérabilités
Oracle		http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujan2008.html	

PLONE

"Cross-Site Scripting" dans 'Plone'

Un manque de validation permet à un utilisateur malicieux de mener des attaques de type "Cross-Site Scripting".

Forte	03/01	Plone 'Plone' version 3.0.3	
Correctif existant		Fonctionnalité 'LiveSearch'	Validation insuffisante des données
Plone		http://dev.plone.org/plone/ticket/7439	

POSTGRESQL

Multiples vulnérabilités dans 'PostgreSQL'

De multiples failles permettent de provoquer un déni de service d'un serveur

Forte	08/01	PostgreSQL 'PostgreSQL' versions 7.3, 7.4, 8.0, 8.1, 8.2	
Correctif existant		Se référer à l'avis original	Erreur de codage
PostgreSQL		http://www.postgresql.org/about/news.905	
CVE-2007-4769, CVE-2007-4772, CVE-2007-6067, CVE-2007-6600, CVE-2007-6601			

PULSEAUDIO

Elévation de privilèges via 'PulseAudio'

Une erreur de codage dans 'PulseAudio' permet à un utilisateur local d'obtenir des droits privilégiés.

Moyenne	25/01	PulseAudio 'PulseAudio' version non disponible	
Correctif existant		Gestion de la fonction 'setuid()'	Erreur de codage
Red Hat Bugzilla		https://bugzilla.redhat.com/show_bug.cgi?id=425481	

SUBLIMATION

Exécution de commandes arbitraires dans 'scponly'

Une faille non documentée dans le produit 'scponly' permet à un attaquant d'exécuter des commandes arbitraires.

Moyenne	22/01	Sublimation 'scponly' version 4.6	
Aucun correctif		Programme 'scp'	Erreur de conception
Debian		http://lists.debian.org/debian-security-announce/debian-security-announce-2008/msg00034.html	

SUN

Multiples vulnérabilités dans Sun			
Des failles permettent de mener d'injecter du code 'HTML' et de rediriger le navigateur vers d'autres sites.			
Forte	17/01	Se référer à l'avis original	
Correctif existant		'Java System Identity Manager'	Non disponible
Sun		http://sunsolve.sun.com/search/document.do?assetkey=1-26-103180-1	

Déni de service dans 'Solaris X Server Extensions'			
De multiples vulnérabilités permettent à un attaquant de provoquer un déni de service.			
Forte	18/01	Sun 'Solaris' versions 8, 9, 10	
Palliatif proposé		Se référer à l'avis original	Multiples vulnérabilités
Sun		http://sunsolve.sun.com/search/document.do?assetkey=1-26-103200-1	
CVE-2007-5760, CVE-2007-6427, CVE-2007-6428, CVE-2007-6429			

Déni de service dans 'Solaris X Window System (X(5))'			
Un manque de validation permet à un attaquant de provoquer un déni de service et d'exécuter du code arbitraire.			
Forte	18/01	Sun 'Solaris' versions 8, 9, 10	
Palliatif proposé		'libfont' et 'libXfont'	Manque de validation
Sun		http://sunsolve.sun.com/search/document.do?assetkey=1-26-103192-1	
CVE-2008-0006			

Elévation de privilèges dans 'Solaris10'			
Une faille permet à un utilisateur local malveillant d'obtenir une élévation de privilèges.			
Forte	14/01	Sun 'Solaris' version 10	
Correctif existant		Bibliothèque 'libdevinfo' (3LIB)	Non disponible
Sun		http://sunsolve.sun.com/search/document.do?assetkey=1-26-103165-1	

Exposition d'informations dans 'Solaris X Server'			
Une faillepermet à un attaquant d'obtenir des informations.			
Forte	18/01	Sun 'Solaris' versions 8, 9, 10	
Palliatif proposé		Options en ligne de commande	Mauvais traitement
Sun		http://sunsolve.sun.com/search/document.do?assetkey=1-26-103205-1	
CVE-2007-5958			

'Kernel panic' dans le système dans 'Solaris 10'			
Une faille permet à un utilisateur local de provoquer une erreur fatale du noyau 'kernel panic'.			
Forte	14/01	Sun 'Solaris' version 10	
Correctif existant		Méthode 'dotoprocs()'	Non disponible
Sun		http://sunsolve.sun.com/search/document.do?assetkey=1-26-103188-1	

Multiples failles dans 'Java System Identity Manager'			
De multiples failles permettent de mener de attaques de type "Cross-Site Scripting".			
Forte	09/01	Sun 'Java System Identity Manager' versions 6.0, 7.0 et 7.1	
Aucun correctif		Non disponible	Non disponible
Sun		http://sunsolve.sun.com/search/document.do?assetkey=1-26-103180-1	

ALERTES NON CONFIRMEES

Les alertes présentées dans les tables de synthèse suivantes ont été publiées dans diverses listes d'information mais n'ont pas encore fait l'objet d'une annonce ou d'un correctif de la part de l'éditeur. Ces alertes nécessitent la mise en place d'un processus de suivi et d'observation.

ADVENTNET

"Cross-Site Scripting" dans 'ManageEngine'			
Des failles permettent d'obtenir des informations et de mener des attaques de type "Cross-Site Scripting".			
Forte	25/01	AdventNet 'ManageEngine Applications Manager' version 8.1 (build 8100)	
Correctif existant		Localisation de cible d'URL	Manque de validation et vérification
Secunia		http://secunia.com/advisories/28332/	

AOL

Exécution de code arbitraire dans 'AOL Radio'			
Un débordement de buffer peut être exploité par un attaquant pour exécuter du code arbitraire.			
Forte	14/01	AOL 'AmpX.dll' versions inférieures à 2.6.2.6	
Aucun correctif		'MediaPlaybackControl.exe'	Débordement de buffer
SecurityFocus		http://www.securityfocus.com/bid/27207	
CVE-2007-6250			

AOL/NULLSOFT

Exécution de code arbitraire dans 'Winamp'

Des débordements de pile dans 'Winamp' permettent de provoquer l'exécution de code arbitraire.

Forte	18/01	AOL/Nullsoft 'Winamp' versions 5.21, 5.5, 5.51	
Correctif existant		Bibliothèque 'in_mp3.dll'	Débordement de pile
Secunia		http://secunia.com/secunia_research/2008-2/advisory	
CVE-2008-0065			

APACHE

"Cross-Site Scripting" dans 'Apache'

Un manque de validation permet à un attaquant de mener des attaques de type "Cross-Site Scripting".

Forte	14/01	Apache 'Apache' versions 2.2.7-dev et inférieures, 1.3.40-dev et 2.0.62-dev	
Aucun correctif		Module 'mod_proxy_ftp'	Manque de validation
SecurityFocus		http://www.securityfocus.com/bid/27234	
CVE-2008-0005			

"Cross-Site Scripting" via 'mod_status'

Un manque de validation permet de mener des attaques de type "Cross-Site Scripting".

Forte	07/01	Apache 'Apache' versions 1.3.2 à 1.3.39, versions 2.0.35 à 2.0.61	
Correctif existant		Module 'mod_status'	Validation insuffisante des données
SecurityTracker		http://securitytracker.com/id?1019154	
CVE-2007-6388			

Exposition d'informations dans 'Tomcat'

Une faille permet à un attaquant d'obtenir des informations dont le cookie 'JSESSIONIDSSO'.

Moyenne	21/01	Apache 'Tomcat' version 5.5.20	
Correctif existant		Valve 'SingleSignOn'	Non disponible
Secunia		http://secunia.com/advisories/28552/	
CVE-2008-0128			

Multiples vulnérabilités dans 'Apache'

De multiples failles permettent de provoquer un déni de service, des corruptions de mémoire.

Forte	14/01	Apache 'Apache' version 2.2.0 et 2.2.2 à 2.2.6	
Correctif existant		Module 'mod_proxy_balancer'	Multiples failles
SecurityFocus		http://www.securityfocus.com/bid/27236/	
CVE-2007-6420, CVE-2007-6421, CVE-2007-6422, CVE-2007-6423			

Failles dans le module Apache 'mod_negotiation'

Des failles permettent de mener des attaques de type "Cross-Site Scripting" et "HTTP Response Splitting".

Moyenne	23/01	Apache 'Apache' versions 1.3.39 et inférieures, 2.0.61 et inférieures et 2.2.6 et inférieures	
Aucun correctif		Module 'mod_negotiation'	Validation insuffisante des données
Minded Security		http://www.mindedsecurity.com/MSA01150108.html	

APPLE

Accès non autorisé dans 'iPhone'

Une faille permet à un utilisateur de contourner la sécurité et d'accéder à des applications non autorisées.

Moyenne	16/01	Apple 'iPhone' versions inférieures à 1.1.3	
Correctif existant		Verrouillage du code PIN	Contournement de la sécurité
SecurityFocus		http://www.securityfocus.com/bid/27297	

Débordement de buffer dans 'QuickTime'

Un débordement de buffer permet de provoquer l'exécution de code arbitraire ou un déni de service.

Forte	10/01	Apple 'QuickTime' version 7.3.1.70	
Aucun correctif		Gestion des flux de type 'RTSP'	Débordement de buffer
SecurityFocus		http://www.securityfocus.com/bid/27225	

Déni de service dans 'QuickTime'

Une corruption de mémoirepermet à un attaquant d'exécuter du code arbitraire et de provoquer un déni de service.

Forte	16/01	Apple 'QuickTime' versions inférieures à 7.4	
Correctif existant		Fichier 'Sorenson 3'	Corruption de mémoire
SecurityFocus		http://www.securityfocus.com/bid/27298	
CVE-2008-0031			

Déni de service dans 'QuickTime' ('IDSC')

Une corruption de mémoire permet à un attaquant d'exécuter du code et de provoquer un déni de service.

Forte	16/01	Apple 'QuickTime' versions inférieures à 7.4	
Correctif existant		'Image Descriptor' (IDSC)	Corruption de mémoire
SecurityFocus		http://www.securityfocus.com/bid/27299	

Déni de service dans 'QuickTime' ('PICT')			
Un débordement de buffer permet à un attaquant d'exécuter du code arbitraire et de provoquer un déni de service.			
Forte	16/01	Apple 'QuickTime' versions inférieures à 7.4	
Correctif existant		Fichier 'PICT'	Débordement de buffer
SecurityFocus		http://www.securityfocus.com/bid/27300	
CVE-2008-0036			

Déni de service via 'Safari' sur 'iPhone'			
Une faille dans le navigateur 'Safari' de l'équipement 'iPhone' permet de provoquer un déni de service de ce produit.			
Forte	24/01	Apple 'iPhone' version 1.1.2	
Aucun correctif		Navigateur 'Safari'	Erreur de conception
SecurityFocus		http://www.securityfocus.com/bid/27442	

Exécution de code arbitraire dans iPhone et iPod Touch			
Une corruption de mémoire permet à un attaquant d'exécuter du code arbitraire.			
Forte	16/01	Apple 'iPhone' versions 1.0 à 1.1.2 et 'iPod Touch' versions 1.1 à 1.1.2	
Correctif existant		Traitement des URLs	Corruption de mémoire
SecurityFocus		http://www.securityfocus.com/bid/27296	
CVE-2008-0035			

Exécution de code arbitraire dans 'QuickTime'			
Un débordement de buffer dans 'QuickTime' permet à un attaquant d'exécuter du code arbitraire.			
Forte	14/01	Apple 'QuickTime' version 7.3.1.70	
Aucun correctif		Protocole 'Real Time Streaming'	Débordement de buffer
SecurityFocus		http://www.securityfocus.com/bid/27225	

Exécution de code arbitraire dans 'QuickTime'			
Une corruption de mémoire dans le produit 'QuickTime' permet à un attaquant d'exécuter du code arbitraire.			
Forte	16/01	Apple 'QuickTime' versions inférieures à 7.4	
Correctif existant		'Macintosh Resource'	Corruption de mémoire
SecurityFocus		http://www.securityfocus.com/bid/27301	
CVE-2008-0032			

ARUBA NETWORKS

Contournement de la sécurité dans les produits Aruba			
Une faille dans l'authentification 'LDAP' permet à un attaquant distant de contourner l'authentification.			
Forte	04/01	Aruba Networks 'Mobility Controllers', se référer à l'avis original	
Correctif existant		Authentification 'LDAP'	Non disponible
Bugtraq		http://marc.info/?l=bugtraq&m=119955401732254&w=2	

BELKIN

Compromission du système dans 'Wireless G Plus MIMO'			
Un contournement de la sécurité permet d'accéder à des fonctionnalités et de compromettre le système.			
Forte	21/01	Belkin 'Wireless G Plus MIMO' version 3.01.53	
Aucun correctif		Non disponible	Contournement de la sécurité
SecurityFocus		http://www.securityfocus.com/bid/27359	

BINTEC

Déni de service dans le routeur 'X2300'			
Une faille non documentée dans le routeur 'X2300' permet à un attaquant de provoquer un déni de service.			
Moyenne	17/01	BINTEC 'X2300' versions inférieures à 7.4.1 Patch 9	
Correctif existant		Requêtes 'DNS'	Non disponible
Secunia		http://secunia.com/advisories/28085/	

BOOST

Déni de service dans 'Boost '			
Un manque de validation dans la bibliothèque 'Boost' permet à un attaquant de provoquer un déni de service.			
Forte	17/01	Boost 'Boost' version 1.33.1	
Aucun correctif		Bibliothèque 'Boost'	Manque de validation
SecurityFocus		http://www.securityfocus.com/bid/27325	

CANDYPRESS

Multiples vulnérabilités dans 'CandyPress'			
Un manque de validation permet de mener des attaques de type "Cross-Site Scripting", d'injecter du code 'SQL'.			
Forte	30/01	CandyPress 'CandyPress Store' version 4.1.1.26	
Correctif existant		Données utilisateur	Manque de validation
SecurityFocus		http://www.securityfocus.com/bid/27454	

CHERRYPY

Exposition d'informations via 'CherryPy'

Une faille dans l'application de développement 'CherryPy' permet d'obtenir des informations.

Moyenne	07/01	CherryPy 'CherryPy' versions 3.0.x et 2.x	
Correctif existant		Gestion des 'cookies'	Erreur de conception
CherryPy		http://www.cherrypy.org/ticket/744	

CISCO

Déni de service dans le client 'VPN' de Cisco

Un mauvais traitement des fichiers 'IOCTL' permet à un utilisateur malveillant de provoquer un déni de service.

Forte	16/01	Cisco 'cvpndrva.sys' version 5.0.02.0090	
Aucun correctif		Fichiers 'IOCTL'	Mauvais traitement
SecurityFocus		http://www.securityfocus.com/bid/27289	

CITRIX

Exécution de code arbitraire dans 'Presentation Server'

Un débordement de buffer dans 'Citrix Presentation Server' permet à un attaquant d'exécuter du code arbitraire.

Forte	17/01	Se référer à l'avis original	
Correctif existant		Service 'IMA'	Débordement de buffer
Secunia		http://secunia.com/advisories/28508/	

CLAMAV

Vulnérabilités dans 'ClamAV'

Plusieurs failles dans l'anti-virus 'ClamAV' permettent de corrompre des fichiers arbitraires ou de contourner l'analyse de certains fichiers par le produit.

Forte	30/12	ClamAV 'ClamAV' version 0.92	
Aucun correctif		Fichier 'libclamav/others.c'	Conflit d'accès aux ressources, Erreur de conception, Gestion des fichiers.
Full Disclosure		http://seclists.org/fulldisclosure/2007/Dec/0625.html	
CVE-2007-6337			

COMODO

Exécution de code via 'Comodo AntiVirus'

Une faille permet de provoquer l'exécution de code arbitraire sur une plate-forme Windows vulnérable.

Forte	23/01	Comodo 'Comodo AntiVirus' version 2.0	
Aucun correctif		Contrôle ActiveX	Erreur de conception
SecurityFocus		http://www.securityfocus.com/bid/27424	

CPANEL

"Cross-Site Scripting" dans 'cPanel'

Un manque de validation permet à un attaquant de mener des attaques de type "Cross-Site Scripting".

Forte	17/01	cPanel 'cPanel'	
Aucun correctif		Fichier 'dohtaccess.html'	Manque de validation
SecurityFocus		http://www.securityfocus.com/bid/27308	

CREATIVE LABS

Elévation de privilèges via le pilote 'es1371mp.sys'

Une faille permet à un utilisateur local d'obtenir des droits privilégiés.

Moyenne	07/01	Creative Labs 'Ensoniq PCI ES1371'	
Aucun correctif		Pilote 'es1371mp.sys'	Erreur de conception
SecurityFocus		http://www.securityfocus.com/bid/27179	

DANSIE

"Cross-Site Scripting" dans Dansie 'Search Engine'

Un manque de validation permet à un attaquant de mener des attaques de type "Cross-Site Scripting".

Forte	15/01	DANSIE 'Search Engine' version 2.7	
Aucun correctif		Fichier 'search.pl'	Manque de validation
SecurityFocus		http://www.securityfocus.com/bid/27269	

"Cross-Site Scripting" dans Dansie 'Photo Album'

Un manque de validation permet à un attaquant de mener des attaques de type "Cross-Site Scripting".

Moyenne	16/01	DANSIE 'Photo Album' version 1.0	
Aucun correctif		Paramètre 'search'	Manque de validation
Secunia		http://secunia.com/advisories/28501/	

DEBIAN

Exécution de code arbitraire dans 'apt-listchanges'

Une erreur de conception dans l'outil 'apt-listchanges' permet à un attaquant d'exécuter du code arbitraire.

Moyenne	18/01	Debian 'apt-listchanges' version 2.82	
Correctif existant		Outil 'apt-listchanges'	Erreur de conception
SecurityFocus		http://www.securityfocus.com/bid/27331	

DIVX

Déni de service via un contrôle ActiveX

Un débordement de buffer permet à un attaquant de provoquer un déni de service sur une plate-forme vulnérable.

Forte	02/01	DivX 'DivX Web Player' version 6.6	
Aucun correctif		Contrôle ActiveX 'npUpload.dll'	Débordement de buffer
SecurityFocus		http://www.securityfocus.com/bid/27106	

ELOG

Multiples failles dans l'application 'Elog'

Deux faillespermettent de provoquer un déni de service et des attaques de type "Cross-Site Scripting".

Moyenne	22/01	Elog 'Elog' versions inférieures à 2.7.1	
Correctif existant		Démon 'elogd'	Validation insuffisante des données en entrée
Secunia		http://secunia.com/advisories/28589/	

ENDIAN

"Cross-Site Scripting" dans 'Endian Firewall'

Un manque de validation permet à un attaquant de mener des attaques de type "Cross-Site Scripting".

Forte	29/01	Endian 'Endian Firewall' version 2.1.2	
Aucun correctif		Données utilisateur	Manque de validation
SecurityFocus		http://www.securityfocus.com/bid/27477	

F5 NETWORKS

"Cross-Site Scripting" dans un produit BIG-IP

Un manque de validation permet à un attaquant distant de mener des attaques de type "Cross-Site Scripting".

Forte	26/01	F5 Networks 'BIG-IP Application Security Manager' version 9.4.3	
Aucun correctif		Interface de gestion	Validation insuffisante des données
SecurityFocus		http://www.securityfocus.com/archive/1/487118	

F5 SOFTWARE

"Cross-Site Scripting" dans F5 'BigIP'

Un manque de validation permet à un attaquant de mener des attaques de type "Cross-Site Scripting".

Forte	15/01	F5 SOFTWARE 'BIG-IP' version 9.4.5	
Aucun correctif		Paramètre 'SearchString'	Manque de validation
SecurityFocus		http://www.securityfocus.com/bid/27272	

FAIL2BAN

Déni de service dans 'Fail2ban'

Un manque de validation dans le produit 'Fail2ban' permet à un attaquant de provoquer un déni de service.

Forte	08/07	fail2ban 'Fail2ban' version 0.8.0 et inférieures	
Aucun correctif		Messages d'erreur	Manque de validation
SecurityFocus		http://www.securityfocus.com/bid/25117	
CVE-2007-4321			

FIREBIRD

Exécution de code arbitraire dans 'Firebird'

Un débordement de buffer permet de provoquer l'exécution de code arbitraire sur une machine vulnérable.

Forte	28/01	Firebird 'Firebird' versions inférieures à 2.1 RC1	
Correctif existant		Noms d'utilisateur	Débordement de buffer
Secunia		http://secunia.com/advisories/28596/	

Exécution de code arbitraire dans 'Firebird'

Un débordement d'entier permet de provoquer l'exécution de code arbitraire sur une plate-forme vulnérable.

Forte	28/01	Se référer à l'avis original	
Correctif existant		Protocole 'XDR'	Débordement d'entier
Core Security		http://www.coresecurity.com/?action=item&id=2095	
CVE-2008-0387			

FORTINET

Contournement de la sécurité dans 'FortiGate'

Une faille permet à un attaquant de contourner la sécurité et d'avoir accès à des sites non autorisés.

Moyenne	15/01	Fortinet 'FortiGate-1000' version 3.00	
Aucun correctif		Caractère 'CRLF'	Mauvaise gestion
SecurityFocus		http://www.securityfocus.com/bid/27276	

FOXIT

Déni de service dans 'Foxit WAC Server'

Une erreur de conception permet à un attaquant de provoquer un déni de service.

Forte	07/01	Foxit 'Foxit WAC Server' version 2.0 build 3503 et version 2.1.0.910	
Aucun correctif		Fichier 'wacsvr.exe'	Erreur de conception
Secunia		http://secunia.com/advisories/28272/	

FREEBSD

Déni de servide dans 'FreeBSD'

Une erreur permet à un attaquant de provoquer un déni de service ou la compromission du système.

Critique	15/01	FreeBSD 'FreeBSD' version 6.2	
Correctif existant		Fonction 'inet_network()'	Débordement de buffer
Secunia		http://secunia.com/advisories/28367/	
CVE-2008-0122			

Exposition d'informations dans 'FreeBSD'

Des erreurs de conception dans 'FreeBSD' permettent à un utilisateur malveillant d'accéder à des informations.

Moyenne	15/01	FreeBSD 'FreeBSD' version 5.0 et inférieures	
Correctif existant		'openpty()' et 'ptsname()'	Erreur de conception
Secunia		http://secunia.com/advisories/28498/	
CVE-2008-0216, CVE-2008-0217			

GE FANUC

Exécution de code arbitraire dans 'CIMPLICITY'

Un débordement de buffer permet à un attaquant distant d'exécuter du code arbitraire.

Forte	30/01	GE Fanuc 'CIMPLICITY' versions inférieures à 7.0 SIM 9	
Correctif existant		Fichier 'w32rtr.exe'	Débordement de buffer
Securityfocus		http://www.securityfocus.com/bid/27447	
CVE-2008-0176			

Exécution de script dans 'Proficy Portal'

Un manque de validation permet à un attaquant d'exécuter du script arbitraire.

Forte	30/01	GE Fanuc 'Proficy Real Time Information Portal' version 2.6	
Aucun correctif		Données utilisateur	Manque de validation
SecurityFocus		http://www.securityfocus.com/bid/27446	
CVE-2008-0175			

Exposition d'informations dans 'Proficy'

Une erreur de conception dans 'Proficy' permet à un attaquant distant d'obtenir des informations.

Forte	30/01	GE Fanuc 'Proficy' version 2.6	
Correctif existant		Non disponible	Erreur de conception
SecurityTracker		http://securitytracker.com/alerts/2008/Jan/1019273.html	
CVE-2008-0174			

GEORGIA SOFTWORKS

Multiples vulnérabilités dans le serveur 'SSH2 Server'

De multiples failles, aux conséquences inconnues, affectent le serveur 'SSH2 Server' de Georgia SoftWorks.

Forte	03/01	Georgia SoftWorks 'SSH2 Server' version 7.01.0003	
Aucun correctif		Fonction de journalisation (	Erreur de chaîne de formatage, Débordement de buffer
Secunia		http://secunia.com/advisories/28307/	

GFORGE

Injection de code 'SQL' dans 'Gforge'

Un manque de validation dans le produit 'GForge' permet à un attaquant d'injecter du code 'SQL'.

Forte	15/01	GForge 'GForge' version 4.5.14, version 3.1, version 4.6	
Aucun correctif		Données utilisateur	Manque de validation
SecurityFocus		http://www.securityfocus.com/bid/27266	
CVE-2008-0173			

GNU

Débordement de buffer dans 'libcdio'

Un manque de validation dans 'libcdio' permet à un attaquant de générer un débordement de buffer.

Moyenne	04/01	Gnu 'libcdio' version 0.79	
Correctif existant		'print_iso9660_recurse()'	Manque de validation
Secunia		http://secunia.com/advisories/28308/	
CVE-2007-6613			

HORDE

Contournement de la sécurité dans les produits Horde

Des failles dans les produits Horde permettent de contourner des mécanismes de sécurité.

Forte	10/01	Se référer à l'avis original	
Correctif existant		Non disponible	Non disponible
SecurityFocus		http://www.securityfocus.com/bid/27217	

Suppression de données dans les produits Horde

Des manques de validation dans des produits Horde permettent de supprimer des données arbitraires.

Forte	10/01	Se référer à l'avis original	
Correctif existant		Gestion 'HTTP' et 'HTML'	Validation insuffisante des données
SecurityFocus		http://www.securityfocus.com/bid/27223	
CVE-2007-6018			

HP

Débordement de buffer via 'Virtual Rooms'

Un contrôle ActiveX du produit HP 'Virtual Rooms' est vulnérable à un débordement de buffer.

N/A	22/01	HP 'Virtual Rooms' version non disponible	
Aucun correctif		Contrôle ActiveX	Débordement de buffer
Full Disclosure		http://lists.grok.org.uk/pipermail/full-disclosure/2008-January/059837.html	

HSQLDB

Faille dans 'hsqldb'

Une faille non documentée aux conséquences inconnues affecte 'hsqldb'.

N/A	25/01	hsqldb 'hsqldb'	
Aucun correctif		Non disponible	Non disponible
Secunia		http://secunia.com/advisories/28585/	
CVE-2007-4576			

IBM

"Cross-Site Scripting" dans 'Lotus Sametime'

Un manque de validation permet à un attaquant de mener des attaques de type "Cross-Site Scripting".

Forte	17/01	IBM 'Lotus Sametime' version 7.5 et version 7.5.1	
Correctif existant		Client 'Sametime'	Manque de validation
Secunia		http://secunia.com/advisories/27942/	

Multiples vulnérabilités dans 'AIX'

De multiples failles permettent d'obtenir une élévation de privilèges et d'exécuter du code, entre autres choses.

Forte	24/01	IBM 'AIX' versions 5.2, 5.3, 6.1, 5.3.7	
Correctif existant		Se référer à l'avis original	Débordement de buffe
Secunia		http://secunia.com/advisories/28609/	
CVE-2007-5764			

Vulnérabilité dans 'WebSphere Application Server'

Une vulnérabilité non documentée, aux conséquences inconnues, affecte 'WebSphere Application Server'.

N/A	22/01	IBM 'WebSphere Application Server' versions 6.0 à 6.0.2.25 et versions 6.1 à 6.1.0.14	
Correctif existant		Se référer à l'avis original	Non disponible
Secunia		http://secunia.com/advisories/28576/	

IRFANVIEW

Corruption de la mémoire dans 'IrfanView'

Une corruption de la mémoire permet de provoquer un déni de service et d'exécuter du code arbitraire.

Forte	28/01	IrfanView 'IrfanView' version 4.10	
Aucun correctif		Gestion fichiers de type 'FPX'	Corruption de la mémoire
SecurityFocus		http://www.securityfocus.com/bid/27479	

ISC BIND

Déni de service dans 'ISC BIND'

Un débordement de buffer permet à un attaquant de provoquer un déni de service.

Forte	21/01	Se référer à l'avis original	
Correctif existant		Fonction 'inet_network()'	Débordement de buffer
Secunia		http://secunia.com/advisories/28579/	
CVE-2008-0122			

LAYTON TECHNOLOGY

"Cross-Site Scripting" dans Layton 'HelpBox'

De multiples failles permettent d'injecter du code 'SQL' ou 'ASP' et de mener des attaques de type "CSS"

Forte	09/01	Layton Technology 'HelpBox' version 3.7.1	
Aucun correctif		Se référer à l'avis original	Manque de validation
Secunia		http://secunia.com/advisories/27699/	
CVE-2007-5401, CVE-2007-5402, CVE-2007-5403, CVE-2007-5404			

LINKSYS

"Cross-Site Request Forgery" dans Linksys 'WRT54GL'

Un manque de validation permet à un attaquant de mener des attaques de type "Cross-Site Request Forgery".

Forte	10/01	Linksys 'WRT54GL' version 4.30.9	
Aucun correctif		Requêtes 'HTTP'	Manque de validation
Secunia		http://secunia.com/advisories/28364	

LINUX

Déni de service dans 'Libxml2'

Une faille non documentée dans la bibliothèque 'Libxml2' permet à un attaquant de provoquer un déni de service.

Forte	14/01	Linux 'Libxml2' versions inférieures à 2.6.31	
Correctif existant		Fonction 'xmlCurrentChar()'	Non disponible
Secunia		http://secunia.com/advisories/28444/	
CVE-2007-6284			

Elévation de privilèges dans le noyau de Linux (2.6)

Une faille permet à un utilisateur local malveillant d'élever ses privilèges et d'avoir accès à des fichiers.

Moyenne	15/01	Linux 'Noyau' version 2.6.23.14	
Correctif existant		Module 'VFS'	Non disponible
SecurityFocus		http://www.securityfocus.com/bid/27280	
CVE-2008-0001			

LUMENSION SECURITY

Elévation de privilèges via 'PatchLink Update'

Une faille permet à un utilisateur local malveillant d'obtenir des droits privilégiés.

Moyenne	28/01	Lumension Security 'PatchLink Update' version non disponible	
Aucun correctif		Se référer à l'avis original	Gestion non sécurisée de fichiers temporaires
SecurityTracker		http://securitytracker.com/id?1019272	

MANSION PRODUCTIONS

Compromission de l'application 'Members Area System'

Un manque de validation permet d'inclure des fichiers à distance et de compromettre ainsi l'application.

Forte	23/01	Mansion Productions 'Member Area System' version 1.7	
Correctif existant		Fichier 'view_func.php'	Manque de validation
SecurityFocus		http://www.securityfocus.com/bid/27244	

MANTIS

"Cross-Site Scripting" dans 'Mantis'

Un manque de validation permet à un attaquant de mener des attaques de type "Cross-Site Scripting".

Forte	28/12	Mantis 'Mantis' version 1.0.8	
Correctif existant		Fichier 'bug_report.php'	Manque de validation
Secunia		http://secunia.com/advisories/28185/	

MARADNS

Déni de service de 'maraDNS'

Une faille permet à un attaquant distant de provoquer un déni de service du produit.

Forte	03/01	MaraDNS 'maraDNS' version 1.0.27, version 1.2.12.04 et version 1.2.12.08	
Aucun correctif		Gestion des paquets DNS	Erreur de codage
SecurityFocus		http://www.securityfocus.com/bid/27124	

MCAFEE

Exécution de code dans McAfee 'E-Business Server'

Une faille permet de provoquer un déni de service d'un serveur ou d'exécuter du code arbitraire.

Forte	09/01	McAfee 'E-Business Server' version 8.5.2 et inférieures	
Correctif existant		Interface d'administration	Non disponible
INfigo		http://www.infigo.hr/en/in_focus/advisories/INFIGO-2008-01-06	
CVE-2008-0127			

MEDIAWIKI

"Cross-Site Scripting" dans 'MediaWiki'

Un manque de validation permet de mener des attaques de type "Cross-Site Scripting".

Forte	21/01	MediaWiki 'MediaWiki' version 1.11 et inférieures	
Aucun correctif		Barre de recherche	Validation insuffisante des données en entrée
SecurityFocus		http://www.securityfocus.com/bid/27370	

MERAK

"Cross-Site Scripting" dans 'IceWarp Mail Server'

Un manque de validation permet à un attaquant distant de mener des attaques de type "Cross-Site Scripting".

Forte	08/01	Merak 'IceWarp Mail Server' version non disponible	
Aucun correctif		Page 'admin/index.html'	Validation insuffisante des données
SecurityFocus		http://www.securityfocus.com/bid/27189	

MICROSOFT

Corruption de données via le contrôle 'richtx32.ocx'

Une faille dans le contrôle ActiveX 'richtx32.ocx' permet de corrompre des données arbitraires à distance.

Moyenne	09/01	Microsoft 'richtx32.ocx' version 6.1.97.82	
Aucun correctif		Gestion de certaines méthodes	Erreur de conception
SecurityFocus		http://www.securityfocus.com/bid/27201	

Exécution de code arbitraire dans Microsoft 'Excel'

Une faille non documentée dans Microsoft 'Excel' permet à un attaquant d'exécuter du code arbitraire.

Forte	16/01	Se référer à l'avis original	
Aucun correctif		Fichier 'Excel'	Non disponible
Secunia		http://secunia.com/advisories/28506/	
CVE-2008-0081			

Exécution de code arbitraire dans 'Visual Basic'

Un débordement de buffer dans 'Visual Basic' de Microsoft permet à un attaquant d'exécuter du code arbitraire.

Forte	21/01	Microsoft 'Visual Basic' version 6.0	
Aucun correctif		Bibliothèque 'MSDE.dll'	Débordement de buffer
Secunia		http://secunia.com/advisories/28563/	

Exécution de code arbitraire dans 'Visual Interdev'

Un débordement de buffer permet à un attaquant d'exécuter du code arbitraire.

Forte	14/01	Microsoft 'Visual InterDev' version 6.0	
Aucun correctif		Fichier 'SLN'	Débordement de buffer
SecurityFocus		http://www.securityfocus.com/bid/27250	

Exécution de commandes via un ActiveX 'Visual FoxPro'

Une faille permet d'exécuter des commandes arbitraires.

Forte	09/01	Microsoft 'Visual FoxPro' version 6.0	
Aucun correctif		ActiveX 'vfp6r.dll'	Erreur de conception
SecurityFocus		http://www.securityfocus.com/bid/27205	

Exécution de commandes via 'VFP_OLE_Server'

Une faille dans le contrôle ActiveX 'VFP_OLE_Server' permet d'exécuter des commandes arbitraires à distance.

Forte	09/01	Microsoft 'VFP_OLE_Server'	
Aucun correctif		ActiveX 'VFP_OLE_Server'	Erreur de conception
SecurityFocus		http://www.securityfocus.com/bid/27199	

Téléchargement de fichiers dans 'Macrovision FLEXnet'

Une faille non documentée dans le produit 'Macrovision FLEXnet' permet à un attaquant de télécharger des fichiers.

Forte	15/01	Microsoft 'Macrovision FLEXnet' version 0	
Aucun correctif		Contrôle ActiveX 'Connect'	Non disponible
SecurityFocus		http://www.securityfocus.com/bid/27279	

MOODLE

"Cross-Site Scripting" dans 'Moodle'

Un manque de validation permet à un attaquant de mener des attaques de type "Cross-Site Scripting".

Forte	14/01	Moodle 'Moodle' versions inférieures à 1.8.4	
Correctif existant		Fichier 'install.php'	Manque de validation
SecurityFocus		http://www.securityfocus.com/bid/27259	
CVE-2008-0123			

MOZILLA

Usurpation de fenêtre dans 'Firefox'

Une faille dans le navigateur 'Firefox' autorise un attaquant à usurper les informations affichées.

Forte	02/01	Mozilla 'Firefox' version 2.0.0.11 et inférieures	
Aucun correctif		Fenêtre d'authentification	Validation insuffisante des données
Aviv Raffon		http://aviv.raffon.net/2008/01/02/YetAnotherDialogSpoofingFirefoxBasicAuthentication.aspx	

Déni de service dans 'Firefox '

Une faille non documentée dans 'Firefox' permet à un attaquant de provoquer un déni de service.

Moyenne	14/01	Mozilla 'Firefox' version 2.0 .10 et inférieures	
Aucun correctif		Non disponible	Non disponible
SecurityFocus		http://www.securityfocus.com/bid/27243	

Exposition d'informations dans 'Firefox'

Sous certaines conditions, une faille dans 'Firefox' permet à un attaquant distant de lire des données arbitraires.

Moyenne	19/01	Mozilla 'Firefox' version 2.0.0.11	
Aucun correctif		Gestion du protocole 'chrome'	Traversée de répertoires
hiredhacker		http://www.hiredhacker.com/2008/01/19/firefox-chrome-url-handling-directory-traversal/	

MYSQL

Déni de service dans 'MySQL'

Un débordement de buffer dans 'MySQL' permet à un attaquant de provoquer un déni de service.

Moyenne	16/01	MySQL 'MySQL' version 5.0.51	
Aucun correctif		Non disponible	Débordement de buffer
Secunia		http://secunia.com/advisories/28419/	
CVE-2008-0226			

NETOPIA

Elévation de privilèges dans 'netOctopus'

Une faille dans l'agent 'netOctopus' permet à un utilisateur local d'obtenir des droits privilégiés.

Forte	07/01	Netopia 'netOctopus' version 5.1.2 build 1011	
Correctif existant		Pilote 'nantsys.sys', interface '\.'	Erreur de conception
iDefense		http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=636	
CVE-2007-5761			

NOVELL

Elévation de privilèges dans 'NetWare Client'

Une faille permet à un utilisateur local d'obtenir des droits privilégiés.

Moyenne	09/01	Novell 'NetWare Client' version 4.91 SP4	
Correctif existant		Pilote 'nicm.sys', interface '\.'	Validation insuffisante des données
iDefense		http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=637	
CVE-2007-5762			

Elévation de privilèges via ZENworks ESM

Une faille autorise un utilisateur à exécuter du script avec des droits privilégiés.

Forte	07/01	Novell 'ZENworks Endpoint Security Management' version 3.5	
Correctif existant		service 'STEngine'	Erreur de conception
iDefense		http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=635	
CVE-2007-5665			

OPENBIBLIO

"Cross-Site Scripting" dans 'OpenBiblio'

Un manque de validation permet de mener d'exécuter du code et d'injecter du code 'SQL', entre autres choses.

Forte	31/12	OpenBiblio 'Openbiblio' version 0.5.2-pre4 et inférieures	
Correctif existant		Données utilisateur	Manque de validation
SecurityFocus		http://www.securityfocus.com/bid/27053	

OPENBSD

Déni de service dans 'OpenBSD'

Une faille dans 'OpenBSD' permet à un utilisateur local malveillant de provoquer un déni de service.

Moyenne	14/01	OpenBSD 'OpenBSD' versions inférieures à 4.2	
Correctif existant		Requêtes 'IOCTL'	Manque de validation
SecurityFocus		http://www.securityfocus.com/bid/27252/	

OPENPEGASUS

Exécution de code arbitraire dans 'OpenPegasus'

Un débordement de buffer dans le produit 'OpenPegasus' permet à un attaquant d'exécuter du code arbitraire.

Forte	08/01	OpenPegasus 'OpenPegasus' version 2.6	
Aucun correctif		Code d'authentification 'PAM'	Débordement de buffer
SecurityFocus		http://www.securityfocus.com/bid/27172	
CVE-2008-0003			

Exécution de code dans 'OpenPegasus'

Un débordement de buffer dans 'OpenPegasus' permet d'exécuter du code arbitraire.

Forte	08/01	OpenPegasus 'OpenPegasus' version 2.x	
Correctif existant		'PAMBasicAuthenticator'	Débordement de buffer
Secunia		http://secunia.com/advisories/28358/	
CVE-2007-5360			

PARAMIKO

Biais dans le générateur aléatoire du module 'paramiko'

Le générateur aléatoire présent dans le module 'paramiko' est biaisé.

Faible	17/01	Paramiko 'paramiko' version 1.7.1	
Correctif existant		Nombre pseudo-aléatoire	Non disponible
SecurityFocus		http://www.securityfocus.com/bid/27307	
CVE-2008-0299			

PEERCAST.ORG

Exécution de code arbitraire dans 'PeerCast'

Un débordement de buffer dans le produit 'PeerCast' permet à un attaquant d'exécuter du code arbitraire.

Forte	31/12	Peercast.org 'PeerCast' version 0.12.17 et versions inférieures à SVN 334	
Correctif existant		Fonction 'HandshakeHTTP'	Débordement de buffer
SecurityFocus		http://www.securityfocus.com/bid/26899	

PHP

Multiples vulnérabilités dans 'PHP'

De multiples failles permettent de provoquer des dénis de service et le contournement de la sécurité.

Forte	03/01	PHP 'PHP' versions inférieures à 4.4.8	
Correctif existant		Se référer à l'avis original	Multiples failles
PHP		http://www.php.net/releases/4_4_8.php	
Secunia		http://secunia.com/advisories/28318/	
CVE-2007-3378			

Contournement de la sécurité dans 'PHP'

Une faille permet de contourner une restriction de sécurité et d'obtenir ainsi l'accès à des fichiers arbitraires.

Moyenne	22/01	PHP 'PHP' version 5.2.4et version 5.2.5	
Correctif existant		Restriction 'safe_mode'	Erreur de conception
SecurityReason		http://securityreason.com/achievement_securityalert/51	
CVE-2007-4850			

PHPBB

"Cross-Site Scripting" dans 'phpBB'

Un manque de validation permet à un attaquant de mener des attaques de type "Cross-Site Scripting".

Forte	03/01	phpBB 'phpBB' version 2.0.22	
Aucun correctif		Données utilisateur	Manque de validation
SecurityFocus		http://www.securityfocus.com/bid/27104	

PHP-NUKE

Injection de code 'SQL' dans 'PHP-Nuke'

Un manque de validation dans 'PHP-Nuke' permet à un attaquant d'injecter du code 'SQL'.

Forte	24/01	PHP-NUKE 'PHP-Nuke' version 8.0	
Aucun correctif		Paramètre 'sid'	Manque de validation
SecurityFocus		http://secunia.com/advisories/28624/	

POSTGRESQL

Exécution de code 'SQL' dans 'PostgreSQL'

Une faille non documentée dans le produit 'PostgreSQL' permet à un attaquant d'exécuter du code 'SQL' arbitraire.

Forte	11/01	PostgreSQL 'PostgreSQL' version 8.1	
Correctif existant		Bibliothèque de lien	Non disponible
Bugtraq		http://www.securityfocus.com/archive/1/archive/1/471541/100/0/threaded	
CVE-2007-3278			

POWERDNS

Contournement de la sécurité dans 'PDNS-Admin'

Une faille permet à un attaquant de contourner la sécurité et ainsi de créer des noms de domaines.

Forte	31/12	PowerDNS 'PDNS-Admin' version 1.1.2	
Correctif existant		Non disponible	Non disponible
SecurityFocus		http://www.securityfocus.com/bid/27036	

RADIUS

Déni de service dans 'Radiator'

Une faille non documentéepermet à un attaquant de provoquer un déni de service.

Forte	17/01	RADIUS 'Radiator' version 3.17.1	
Correctif existant		Non disponible	Non disponible
SecurityFocus		http://www.securityfocus.com/bid/27306	

REAL NETWORKS

Exécution de code arbitraire dans 'RealPlayer'

Un débordement de buffer permet de provoquer l'exécution de code arbitraire ou un déni de service.

Forte	01/01	Real Networks 'RealPlayer' version 11	
Aucun correctif		Non disponible	Débordement de buffer
SecurityFocus		http://www.securityfocus.com/bid/27091	

Débordement de tas dans 'Helix Server'

Un débordement de tas permet d'exécuter du code arbitraire ou un déni de service.

Forte	03/01	Real Networks 'Helix Server' versions 11.1.2, 11.1.4, 11.1.6	
Aucun correctif		Non disponible	Débordement de tas
SecurityFocus		http://www.securityfocus.com/bid/27122	

SAP

Exécution de commandes via 'MaxDB'

Une faille permet à un utilisateur distant d'exécuter des commandes arbitraires sur une base vulnérable.

Forte	09/01	SAP 'MaxDB' version 7.6.03 build 007 et inférieures	
Aucun correctif		Commande 'exec_sdbinfo'	Erreur de conception
SecurityTracker		http://securitytracker.com/id?1019171	

SDL

Débordement de buffer dans 'SDL_image'

Un débordement de buffer permet de provoquer un déni de service ou l'exécution potentielle de code arbitraire.

Forte	23/01	SDL 'SDL_image' version 1.2.6 et inférieures	
Correctif existant		Gestion des images 'GIF'	Débordement de buffer
SecurityFocus		http://www.securityfocus.com/bid/27417	

SKYPE

Exécution de code arbitraire dans 'Skype'

Une faille dans l'application 'Skype' permet à un attaquant d'exécuter du code arbitraire.

Forte	18/01	Skype 'Skype' version 3.6.0.244	
Aucun correctif		'Web content Zones'	Mauvaise utilisation
SecurityFocus		http://www.securityfocus.com/bid/27338	

SOFTWIN

Exposition d'informations dans 'BitDefender'

Une traversée de répertoire permet à un attaquant distant d'obtenir des informations sensibles.

Forte	21/01	Softwin 'BitDefender Enterprise Manager' version 0 et 'BitDefender Security for File Servers' version 0	
Aucun correctif		Démon 'HTTP'	Traversée de répertoire
SecurityFocus		http://www.securityfocus.com/bid/27358	

SSH.COM

Elévation de privilèges dans 'SSH Tectia'

Une faille non documentée permet à un utilisateur local malveillant d'obtenir une élévation de privilèges.

Moyenne	09/01	SSH.COM 'SSH Tectia' versions 5.0 à 5.2.3 et versions 5.3 à 5.3.5	
Correctif existant		Non disponible	Non disponible
SecurityFocus		http://www.securityfocus.com/bid/27191	
CVE-2007-5616			

SUN

Déni de service dans le produit Sun 'JRE'

Un déréférencement de pointeur NULL dans le produit Sun 'JRE' permet de provoquer un déni de service.

Forte	08/01	Sun 'JRE' versions inférieures à 5.0 update 14	
Correctif existant		Bibliothèque 'jpiexp32.dll'	Déréférencement de pointeur NULL
Bugtraq		http://marc.info/?l=bugtraq&m=119980706302163&w=2	
CVE-2007-0012			

SYNCE

Injection de commandes arbitraires dans 'SynCE'

Une faille permet à un attaquant distant d'injecter et d'exécuter des commandes arbitraires.

Moyenne	09/01	SynCE 'Synce-dccm' version 0.92 et inférieures	
Correctif existant		démon 'vdccm'	Validation insuffisante des données
Core Security		http://www.coresecurity.com/index.php5?module=ContentMod&action=item&id=2070	

TOSHIBA

Débordement de pile dans 'Surveillix RecordSend'

Un débordement de buffer permet à un attaquant de générer un débordement de pile.

Forte	22/01	Toshiba 'Surveillix RecordSend Class ActiveX' version 1.0.0.4	
Aucun correctif		Contrôle ActiveX	Débordement de buffer
Secunia		http://secunia.com/advisories/28557/	

TRIPWIRE

"Cross-Site Scripting" dans Tripwire Enterprise/Server

Un manque de validation permet à un attaquant distant de mener des attaques de type "Cross-Site Scripting".

Forte	29/01	TripWire 'Tripwire Enterprise/Server' version 7.0	
Aucun correctif		Page d'authentification	Validation insuffisante des données
Bugtraq		http://www.securityfocus.com/archive/1/487229	

TROLLTECH

Usurpation de certificat dans 'Qt'

Une erreur de conception dans le produit 'Qt' permet à un attaquant d'usurper des certificats.

Forte	03/01	Trolltech 'Qt' versions 4.3.0, 4.3.1, 4.3.2	
Correctif existant		Certificat de validation	Erreur de conception
Secunia		http://secunia.com/advisories/28228/	
CVE-2007-5965			

TUTOS

Exécution de code arbitraire dans 'TUTOS'

Des failles dans 'TUTOS' permettent à un attaquant d'exécuter du code arbitraire et d'obtenir des informations.

Forte	09/01	TUTOS 'TUTOS' version 1.3.20070317	
Aucun correctif		Scripts	Restrictions trop laxistes
Secunia		http://secunia.com/advisories/28291/	

UNP

Exécution de commandes arbitraires via 'unp'

Un manque de validation des noms d'archives permet d'exécuter du code arbitraire sur une machine vulnérable.

Moyenne	10/01	unp 'unp' versions inférieures à 1.0.14	
Correctif existant		Gestion des noms de fichiers	Validation insuffisante des données
Secunia		http://secunia.com/advisories/28282	
CVE-2007-6610			

VIDEOLAN

Exécution de code arbitraire dans 'VLC'

Un débordement de taspermet d'exécuter du code arbitraire sur une plate-forme vulnérable.

Forte	10/01	VideoLAN 'VLC' version 0.8.6d et inférieures	
Aucun correctif		Fichier	Débordement de tas

WEBEVENT

"Cross-Site Scripting" dans 'WebEvent'

Un manque de validation permet à un attaquant de mener des attaques de type "Cross-Site Scripting".

Forte	14/01	WEBEVENT 'WebEvent'	
Aucun correctif		Paramètre 'cmd'	Manque de validation
Secunia		http://secunia.com/advisories/28389/	

WORDPRESS

"Cross-Site Scripting" dans 'Permalinks Migration'

Un manque de vérification permet à un attaquant de mener des attaques de type "Cross-Site Scripting".

Forte	25/01	WordPress 'Permalinks Migration' version 1.0	
Aucun correctif		Requêtes 'HTTP'	Manque de vérification
Secunia		http://secunia.com/advisories/28593/	

"Cross-Site Scripting" dans 'WordPress'

Des manques de validation permettent de mener des attaques de type "Cross-Site Scripting".

Forte	03/01	WordPress 'WordPress' version 2.2.3 et inférieures	
Aucun correctif		Scripts	Validation insuffisante des données
SecurityFocus		http://www.securityfocus.com/bid/27123	

Injection de code 'SQL' dans 'WordPress'

Un manque de validation permet à un attaquant d'injecter du code arbitraire.

Forte	22/01	WordPress 'WordPress' version 1.7.4	
Aucun correctif		Paramètre 'user'	Manque de validation
Secunia		http://secunia.com/advisories/28567/	

Modification de données dans le greffon 'fGallery'

Une injection de code 'SQL' permet à un attaquant de modifier des données et de compromettre l'application.

Moyenne	29/01	WordPress 'fGallery' version 2.4.1	
Aucun correctif		Greffon 'fGallery'	Injection de code 'SQL'
SecurityFocus		http://www.securityfocus.com/bid/27464	

Modification de données dans le greffon 'wp-AdServe'

Une injection de code 'SQL' permet à un attaquant de modifier des données et de compromettre l'application.

Moyenne	30/01	WordPress 'wp-AdServe' version 0.2	
Aucun correctif		Greffon 'wp-AdServe'	Injection de code 'SQL'
SecurityFocus		http://www.securityfocus.com/bid/27504	

Modification de données dans le greffon 'WP-Cal'

Une injection de code 'SQL' permet à un attaquant de modifier des données et de compromettre l'application.

Moyenne	29/01	WordPress 'WP-Cal' version 0.3	
Aucun correctif		Greffon 'WP-Cal'	Injection de code 'SQL'
SecurityFocus		http://www.securityfocus.com/bid/27465	

XENSOURCE

Déni de service dans 'Xen'

Des failles dans les registres 'DR7' et 'CR4' permettent à un utilisateur malveillant de provoquer un déni de service.

Forte	10/01	XenSource 'Xen' version 3.x	
Aucun correctif		Registre de "debug" 'DR7'	Manque de vérification
Secunia		http://secunia.com/advisories/28405/	
CVE-2007-5906, CVE-2007-5907			

XINE

Débordement de tas dans 'xine-lib'

Un débordement de tas dans 'xine-lib' permet d'exécuter potentiellement du code arbitraire ou un déni de service.

Forte	09/01	Xine 'xine-lib' version 1.1.9	
Aucun correctif		Fichier 'input/libreal/rmff.c'	Débordement de tas
Secunia		http://secunia.com/advisories/28384/	

XMP

Exécution de code arbitraire dans Extended Media Player

Des débordements de buffer permettent à un attaquant d'exécuter du code arbitraire.

Forte	31/12	xmp 'Extended Media Player' version 2.5.1	
Aucun correctif		Fichiers 'oxm.c' et 'dtt_load.c'	Débordement de buffer
SecurityFocus		http://www.securityfocus.com/bid/27047	

X.ORG

Exposition d'informations dans X.Org ' X Server'			
De multiples failles permettent d'obtenir une élévation de privilèges, des informations et d'exécuter du code.			
Forte	18/01	X.Org 'X Server'	
Correctif existant		Non disponible	Non disponible
SecurityFocus		http://www.securityfocus.com/bid/27336	
CVE-2007-5760, CVE-2007-5958, CVE-2007-6427, CVE-2007-6428, CVE-2007-6429, CVE-2008-0006			

YABB

Exposition d'informations dans 'YaBB SE'			
Un contournement de la sécurité permet de compromettre l'application et d'exécuter du script.			
Forte	24/01	YABB 'YaBB SE' version 1.5.5 et inférieures	
Aucun correctif		Informations d'authentification	Contournement de sécurité
SecurityFocus		http://www.securityfocus.com/bid/27414	

YARSSR

Injection de code dans 'Yarssr'			
Une faille dans 'Yarssr' permet d'injecter et d'exécuter du code arbitraire sur une plate-forme vulnérable.			
Forte	28/01	Yarssr 'Yarssr' version 0.2.2	
Aucun correctif		Bibliothèque 'GUI.PM'	Validation insuffisante des données
SecurityFocus		http://www.securityfocus.com/bid/26273	
CVE-2007-5837			

YASSL

Exécution de code arbitraire dans 'yaSSL'			
Un débordement de buffer dans 'yaSSL' permet à un attaquant d'exécuter du code arbitraire.			
Forte	29/01	yaSSL 'yaSSL' version 1.7.5	
Correctif existant		Non disponible	Débordement de buffer
SecurityFocus		http://www.securityfocus.com/bid/27140	
CVE-2008-0226, CVE-2008-0227			

AUTRES INFORMATIONS

REPRISES D'AVIS ET CORRECTIFS

Les vulnérabilités suivantes, déjà publiées, ont été mises à jour, reprises par un autre organisme ou ont donné lieu à la fourniture d'un correctif:

AVAYA

"Cross-Site Scripting" dans Avaya ('HTTP')
Des failles dans les produits Avaya permettent à un attaquant de mener des attaques de type "Cross-Site Scripting". Ces failles sont similaires à celles précédemment discutées pour Apache.
http://secunia.com/advisories/28607/
CVE-2007-4465, CVE-2007-5000, CVE-2007-6388, CVE-2008-0005

Déni de service dans Avaya 'CMS'
Des failles dans Avaya 'CMS' (Call Management System) versions R12, R13/13.1 et R14 permettent à un attaquant de provoquer un déni de service. Ces failles sont similaires à celles précédemment discutées pour Sun 'Solaris'.
http://secunia.com/advisories/28693/
CVE-2007-5760, CVE-2007-6427, CVE-2007-6428, CVE-2007-6429

Déni de service dans Avaya 'CMS/IR' ('Sun Solaris')
Une faille dans Avaya 'CMS/IR' permet à un attaquant de provoquer un déni de service. Cette faille est similaire à celle précédemment discutée pour Sun Solaris.
http://secunia.com/advisories/28621/
CVE-2008-0006

Déni de service dans Avaya ('e2fsprogs')
Une faille dans Avaya permet à un attaquant de provoquer un déni de service. Cette faille est similaire à celle précédemment discutée pour 'e2fsprogs'.
http://secunia.com/advisories/27889/
CVE-2007-5497

Elévation de privilèges dans Avaya ('util-linux')
Une faille dans les commandes 'mount' et 'umount' de 'util-linux' affecte les produits Avaya. Cette faille permet à un utilisateur local d'élever ses privilèges. Cette faille est similaire à celle précédemment discutée pour 'util-linux'.
http://secunia.com/advisories/28469/
CVE-2007-5191

Exécution de code arbitraire dans Avaya ('Perl')

Une faille dans les produits 'Perl' affecte les produits Avaya. Cette faille, une erreur de conception dans le moteur d'expression régulière de 'Perl', autorise un utilisateur local malveillant à exécuter du code arbitraire.

http://secunia.com/advisories/28387/

CVE-2007-5116

Multiples vulnérabilités dans Avaya ('OpenSSH')

Des failles dans le produit 'OpenSSH' affectent les produits Avaya. Ces failles permettent à un attaquant d'obtenir des informations, de provoquer un déni de service, d'exécuter du code arbitraire et d'injecter des données arbitraires dans un fichier de journalisation. Ces failles sont similaires à celles précédemment discutées pour 'OpenSSH'.

http://secunia.com/advisories/28320/

CVE-2006-5052, CVE-2007-3102

Vulnérabilités dans Avaya ('pam' et 'OpenSSH')

Des failles dans les produits 'pam' et 'OpenSSH' affectent les produits Avaya. Ces failles permettent à un attaquant d'injecter des données arbitraires dans un fichier de journalisation et d'obtenir des privilèges d'autres utilisateurs. Ces failles sont similaires à celles précédemment discutées pour 'pam' et 'OpenSSH'.

http://secunia.com/advisories/28319/

CVE-2007-1716, CVE-2007-3102

CIAC

Reprise de l'alerte 27454

Le CIAC a repris, sous la référence S-138, l'alerte 27454 concernant de multiples failles dans 'CandyPress' qui permettent de mener des attaques de type "Cross-Site Scripting", entre autres choses.

http://www.ciac.org/ciac/bulletins/s-138.shtml

Reprise de l'alerte Apache ('httpd')

Le CIAC a repris, sous la référence S-118, l'alerte Apache ('httpd') concernant de multiples failles qui permettent de provoquer un déni de service et autorisent un attaquant à mener des attaques de type "Cross-Site Scripting".

http://www.ciac.org/ciac/bulletins/s-118.shtml

CVE-2007-5000, CVE-2007-6388, CVE-2007-6421, CVE-2007-6422

Reprise de l'alerte BIND

Le CIAC a repris, sous la référence S-131, la vulnérabilité BIND référencée CVE-2008-0122 qui permet de provoquer un déni de service d'un serveur vulnérable.

http://www.ciac.org/ciac/bulletins/s-131.shtml

CVE-2008-0122

Reprise de l'alerte Cisco 100345

Le CIAC a repris, sous la référence S-122, l'alerte Cisco 100345 concernant un débordement de buffer dans 'Cisco Unified Communications Manager' qui permet à un attaquant d'exécuter du code et de provoquer un déni de service.

http://www.ciac.org/ciac/bulletins/s-122.shtml

CVE-2008-0027

Reprise de l'alerte Debian DSA-1438

Le CIAC a repris, sous la référence S-100, l'alerte Debian DSA-1438 concernant la disponibilité de correctifs pour le paquetage 'tar' sur Debian GNU/Linux version 4.0 (etch). Ils corrigent de multiples failles qui permettent de provoquer un déni de service et de mener des attaques de type traversées de répertoire.

http://www.ciac.org/ciac/bulletins/s-100.shtml

CVE-2007-4131, CVE-2007-4476

Reprise de l'alerte Debian DSA-1439

Le CIAC a repris, sous la référence S-102, l'alerte Debian DSA-1439 concernant la disponibilité de correctifs pour le paquetage 'typo3-src' sur Debian GNU/Linux version 4.0 (etch). Ils corrigent une faille dans le produit 'TYPO3' qui permet à un attaquant distant d'injecter du code 'SQL'.

http://www.ciac.org/ciac/bulletins/s-102.shtml

CVE-2007-6381

Reprise de l'alerte Debian DSA-1441

Le CIAC a repris, sous la référence S-099, l'alerte Debian DSA-1441 concernant la disponibilité de correctifs pour le paquetage 'peercast' sur Debian GNU/Linux version 4.0 (etch). Ils corrigent un débordement de buffer dans le produit 'PeerCast' qui permet à un attaquant d'exécuter du code arbitraire.

http://www.ciac.org/ciac/bulletins/s-099.shtml

CVE-2007-6454

Reprise de l'alerte Debian DSA-1442

Le CIAC a repris, sous la référence S-104, l'alerte Debian DSA-1442 concernant la disponibilité de correctifs pour le paquetage 'libsndfile' sur Debian GNU/Linux version 4.0 (etch). Ils corrigent un débordement de buffer dans 'libsndfile' qui permet d'exécuter du code arbitraire dans les applications utilisant cette bibliothèque.

http://www.ciac.org/ciac/bulletins/s-104.shtml

CVE-2007-4974

Reprise de l'alerte Debian DSA-1446

Le CIAC a repris, sous la référence S-103, l'alerte Debian DSA-1446 concernant la disponibilité de correctifs pour le paquetage 'wireshark' sur Debian GNU/Linux version 4.0 (etch). Ils corrigent de multiples failles dans l'outil réseau 'Wireshark' qui permettent de provoquer un déni de service du produit ou de la plate-forme vulnérable.

http://www.ciac.org/ciac/bulletins/s-103.shtml

CVE-2007-6450, CVE-2007-6451

Reprise de l'alerte Debian DSA-1457

Le CIAC a repris, sous la référence S-114, l'alerte Debian DSA-1457 concernant la disponibilité de correctifs pour le paquetage 'dovecot' sur Debian GNU/Linux version 4.0 (etch). Ils corrigent une erreur de conception dans l'authentification 'LDAP' de 'Dovecot' qui permet à un utilisateur d'obtenir les droits d'un autre utilisateur.

http://www.ciac.org/ciac/bulletins/s-114.shtml

CVE-2007-6598

Reprise de l'alerte Debian DSA-1458

Le CIAC a repris, sous la référence S-110, l'alerte Debian DSA-1458 concernant la disponibilité de correctifs pour le paquetage 'openafs' sur Debian GNU/Linux versions 3.1 (sarge) et 4.0 (etch). Ils corrigent une faille dans 'OpenAFS' qui permet de provoquer un déni de service d'un serveur vulnérable.

http://www.ciac.org/ciac/bulletins/s-110.shtml

CVE-2007-6599

Reprise de l'alerte Debian DSA-1465

Le CIAC a repris, sous la référence S-119, l'alerte Debian DSA-1465 concernant la disponibilité de correctifs pour le paquetage 'apt-listchanges' sur Debian GNU/Linux version 4.0 (etch). Ils corrigent une erreur de conception dans l'outil 'apt-listchanges' qui permet à un attaquant d'exécuter du code arbitraire.

http://www.ciac.org/ciac/bulletins/s-119.shtml

CVE-2008-0302

Reprise de l'alerte Debian DSA-1467

Le CIAC a repris, sous la référence S-129, l'alerte Debian DSA-1467 concernant la disponibilité de correctifs pour le paquetage 'mantis' sur Debian GNU/Linux versions 3.1 (sarge) et 4.0 (etch). Ils corrigent un manque de validation dans le produit 'Mantis' qui permet à un attaquant de mener des attaques de type "Cross-Site Scripting".

http://www.ciac.org/ciac/bulletins/s-129.shtml

CVE-2006-6574, CVE-2007-6611

Reprise de l'alerte GE Fanuc KB12458

Le CIAC a repris, sous la référence S-132, l'alerte GE Fanuc KB12458 concernant de multiples failles dans des produits GE Fanuc qui permettent de provoquer un déni de service ou l'exécution de code arbitraire.

http://www.ciac.org/ciac/bulletins/s-132.shtml

CVE-2008-0174, CVE-2008-0175, CVE-2008-0176

Reprise de l'alerte HP HPSBGN02301 (SSRT071508)

Le CIAC a repris, sous la référence S-107, l'alerte HP HPSBGN02301 (SSRT071508) concernant une faille dans le contrôle ActiveX 'RulesEngine.dll'. Cette faille peut être exploitée à distance afin d'exécuter du code arbitraire ou d'obtenir des droits privilégiés sur une plate-forme Windows vulnérable.

http://www.ciac.org/ciac/bulletins/s-107.shtml

CVE-2007-6506

Reprise de l'alerte HP HPSBMA02239 (SSRT061260)

Le CIAC a repris, sous la référence S-111, l'alerte HP HPSBMA02239 (SSRT061260) concernant de multiples débordements de buffer dans les produits HP 'OpenView' qui peuvent permettre à un attaquant distant d'exécuter du code arbitraire.

http://www.ciac.org/ciac/bulletins/s-111.shtml

CVE-2007-3872

Reprise de l'alerte HP HPSBUX02295 (SSRT071333)

Le CIAC a repris, sous la référence S-098, l'alerte HP HPSBUX02295 (SSRT071333) concernant une faille non documentée dans le système d'exploitation 'HP-UX' qui permet à un attaquant de provoquer un déni de service.

http://www.ciac.org/ciac/bulletins/s-098.shtml

CVE-2007-6419

Reprise de l'alerte HP HPSBUX02303 (SSRT071468)

Le CIAC a repris, sous la référence S-116, l'alerte HP HPSBUX02303 (SSRT071468) concernant la disponibilité de correctifs pour 'HP-UX'. Ils corrigent deux failles qui affectent le composant 'xfs' ('X Font Server') du serveur X Window 'X.Org' et permettent de provoquer l'exécution de code arbitraire avec les droits associés à 'xfs'.

http://www.ciac.org/ciac/bulletins/s-116.shtml

CVE-2007-4990

Reprise de l'alerte Microsoft MS08-001

Le CIAC a repris, sous la référence S-105, l'alerte Microsoft MS08-001 concernant deux failles dans la pile 'TCP/IP' des plate-formes Windows qui permettent de provoquer des dénis de service et l'exécution de code arbitraire.

http://www.ciac.org/ciac/bulletins/s-105.shtml

CVE-2007-0066, CVE-2007-0069

Reprise de l'alerte Microsoft MS08-002

Le CIAC a repris, sous la référence S-106, l'alerte Microsoft MS08-002 concernant une faille dans le processus 'LSASS' des plate-formes Windows qui permet à un utilisateur local d'obtenir des droits privilégiés.

http://www.ciac.org/ciac/bulletins/s-106.shtml

CVE-2007-5352

Reprise de l'alerte Oracle Janvier 2008

Le CIAC a repris, sous la référence S-117, l'alerte Oracle de Janvier 2008 concernant de multiples vulnérabilités dans les produits Oracle qui peuvent entraîner de nombreuses conséquences.

http://www.ciac.org/ciac/bulletins/s-117.shtml

Reprise de l'alerte Red Hat RHSA-2008:0002

Le CIAC a repris, sous la référence S-113, l'alerte Red Hat RHSA-2008:0002 concernant la disponibilité de correctifs pour le paquetage 'tog-pegasus' sur Red Hat Enterprise Linux 4 et 5. Ils corrigent un débordement de buffer dans le produit 'OpenPegasus' qui permet à un attaquant d'exécuter du code arbitraire.

http://www.ciac.org/ciac/bulletins/s-113.shtml

CVE-2008-0003

Reprise de l'alerte Red Hat RHSA-2008:0029

Le CIAC a repris, sous la référence S-124, l'alerte Red Hat RHSA-2008:0029 concernant la disponibilité de correctifs pour le paquetage 'XFree86' sur Red Hat Enterprise Linux 2.1 et 3. Ils corrigent de multiples failles qui permettent à un attaquant d'obtenir une élévation de privilèges, des informations et d'exécuter du code arbitraire.

http://www.ciac.org/ciac/bulletins/s-124.shtml

CVE-2007-4568, CVE-2007-4990, CVE-2007-5958, CVE-2007-6427, CVE-2007-6428, CVE-2007-6429, CVE-2008-0006

Reprise de l'alerte Red Hat RHSA-2008:0031

Le CIAC a repris, sous la référence S-123, l'alerte Red Hat RHSA-2008:0031 concernant la disponibilité de correctifs pour le paquetage 'xorg-x11-server' sur Red Hat Enterprise Linux 5. Ils corrigent de multiples failles non documentées dans X.Org 'X Server' qui permettent à un attaquant d'obtenir une élévation de privilèges, des informations et d'exécuter du code arbitraire.

http://www.ciac.org/ciac/bulletins/s-123.shtml

CVE-2007-5760, CVE-2007-5958, CVE-2007-6427, CVE-2007-6428, CVE-2007-6429

Reprise de l'alerte Red Hat RHSA-2008:0038

Le CIAC a repris, sous la référence S-108, l'alerte Red Hat RHSA-2008:0038 concernant la disponibilité de correctifs pour le paquetage 'postgresql' sur Red Hat Enterprise Linux 4 et 5. Ils corrigent de multiples failles dans la base de données 'PostgreSQL' qui permettent de provoquer un déni de service d'un serveur ou autorisent un utilisateur malveillant à obtenir des droits privilégiés, entre autres choses.

http://www.ciac.org/ciac/bulletins/s-108.shtml

CVE-2007-3278, CVE-2007-4769, CVE-2007-4772, CVE-2007-6067, CVE-2007-6600, CVE-2007-6601

Reprise de l'alerte Security Focus 27244

Le CIAC a repris, sous la référence S-126, l'alerte Security Focus 27244 concernant un manque de validation dans 'Members Area System' (MAS) qui permet à un attaquant d'inclure des fichiers à distance et de compromettre ainsi l'application.

http://www.ciac.org/ciac/bulletins/s-126.shtml

Reprise de l'alerte Security Focus 27280

Le CIAC a repris, sous la référence S-121, l'alerte Security Focus 27280 concernant une faille non documentée dans le noyau de Linux qui permet à un utilisateur local malveillant d'élever ses privilèges et d'avoir accès à des fichiers.

http://www.ciac.org/ciac/bulletins/s-121.shtml

CVE-2008-0001

Reprise de l'alerte Security Focus 27329

Le CIAC a repris, sous la référence S-125, l'alerte Security Focus 27329 concernant un débordement de buffer dans 'Citrix Presentation Server' qui permet à un attaquant d'exécuter du code arbitraire.

http://www.ciac.org/ciac/bulletins/s-125.shtml

Reprise de l'alerte SecurityFocus 27455

Le CIAC a repris, sous la référence S-136, l'alerte SecurityFocus 27455 concernant deux failles dans la bibliothèque 'ICU' qui permettent de provoquer l'exécution de code arbitraire.

http://www.ciac.org/ciac/bulletins/s-136.shtml

CVE-2007-4770, CVE-2007-4771

Reprise de l'alerte US-CERT VU#112179

Le CIAC a repris, sous la référence S-109, l'alerte US-CERT VU#112179 concernant un débordement de buffer dans 'QuickTime' qui permet à un attaquant d'exécuter du code arbitraire.

http://www.ciac.org/ciac/bulletins/s-109.shtml

Reprise de l'alerte US-CERT VU#249337

Le CIAC a repris, sous la référence S-101, l'alerte US-CERT VU#249337 concernant une faille non documentée dans les produits 'Dreamweaver' et 'Acrobat Connect' d'Adobe qui permet à un attaquant de mener des attaques de type "Cross-Site Scripting".

http://www.ciac.org/ciac/bulletins/s-101.shtml

Reprise de l'alerte US-CERT VU#347812

Le CIAC a repris, sous la référence S-120, l'alerte US-CERT VU#347812 concernant une corruption de la mémoire sur les plate-formes 'Windows XP' qui peut permettre à un attaquant distant d'exécuter du code arbitraire sur une machine vulnérable.

http://www.ciac.org/ciac/bulletins/s-120.shtml

CVE-2007-1204

Reprise de l'alerte US-CERT VU#568681

Le CIAC a repris, sous la référence S-115, l'alerte US-CERT VU#568681 concernant un débordement de buffer dans le produit 'AOL Radio' qui peut être exploité par un attaquant pour exécuter du code arbitraire.

http://www.ciac.org/ciac/bulletins/s-115.shtml

CVE-2007-6250

Reprise de l'alerte US-CERT VU#921339

Le CIAC a repris, sous la référence S-112, l'alerte US-CERT VU#921339 concernant une faille non documentée dans le client et le serveur de 'SSH Tectia' qui permet à un utilisateur local malveillant d'obtenir une élévation de privilèges.

http://www.ciac.org/ciac/bulletins/s-112.shtml

CVE-2007-5616

Reprise de l'avis Debian DSA-1469

Le CIAC a repris, sous la référence S-134, l'avis Debian DSA-1469 concernant des failles dans la bibliothèque 'libFLAC' qui permettent à un attaquant distant de générer un débordement de buffer et d'exécuter du code arbitraire, entre autres choses.

http://www.ciac.org/ciac/bulletins/s-134.shtml

CVE-2007-4619, CVE-2007-6277

Reprise de l'avis Debian DSA-1471

Le CIAC a repris, sous la référence S-135, l'avis Debian DSA-1471 concernant de multiples failles dans la bibliothèque 'libvorbis' qui permettent de provoquer des dénis de service des applications l'utilisant ou la corruption de la mémoire d'une plate-forme vulnérable.

http://www.ciac.org/ciac/bulletins/s-135.shtml

CVE-2007-3106, CVE-2007-4029, CVE-2007-4066

Reprise de l'avis Debian DSA-1472

Le CIAC a repris, sous la référence S-133, l'avis Debian DSA-1472 concernant une faille dans la bibliothèque 'xine-lib' qui permet d'exécuter potentiellement du code arbitraire ou un déni de service.

http://www.ciac.org/ciac/bulletins/s-133.shtml

CVE-2008-0225

Reprise de l'avis Debian DSA-1477

Le CIAC a repris, sous la référence S-137, l'avis Debian DSA-1477 concernant une faille dans 'yarssr' qui permet d'injecter et d'exécuter du code arbitraire.

http://www.ciac.org/ciac/bulletins/s-137.shtml

CVE-2007-5837

Reprise de l'avis SecurityFocus 27399

Le CIAC a repris, sous la référence S-130, le bulletin SecurityFocus 27399 concernant deux failles dans le produit 'Elog' qui permettent de provoquer un déni de service et autorisent un attaquant à mener des attaques de type "Cross-Site Scripting".

http://www.ciac.org/ciac/bulletins/s-130.shtml

CISCO

Révision du bulletin 100389 (cisco-sa-20071219-fwsm)

Cisco a révisé le bulletin 100389 (cisco-sa-20071219-fwsm) concernant une vulnérabilité dans Cisco 'Firewall Services Module' qui permet de provoquer un redémarrage d'un équipement vulnérable. Cette révision annonce la disponibilité d'une nouvelle version corrigeant ce problème durant la semaine du 7 janvier 2008.

http://www.cisco.com/warp/public/707/cisco-sa-20071219-fwsm.shtml

CVE-2007-5584

Révision du bulletin 50961

Cisco a révisé le bulletin 50961 concernant la vulnérabilité de certains équipements à une attaque par déni de service. Cette révision met à jour la liste des produits affectés, ainsi que les versions corrigeant cette faille pour certains produits.

http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml

CLAMAV

Code d'exploitation pour la faille CVE-2007-6335

Un code a été publié sur le site Web Milw0rm exploitant la faille 'ClamAV' référencée CVE-2007-6335. Elle permet d'exécuter du code arbitraire. Ce code permet de générer un exécutable malicieux permettant de déclencher la vulnérabilité, autorisant ainsi à obtenir un interpréteur de commandes à distance sur le port TCP/4444.

http://milw0rm.com/exploits/4862

CVE-2007-6335

FREEBSD

Disponibilité de plusieurs correctifs

FreeBSD annonce la disponibilité des correctifs corrigeant les vulnérabilités présentes dans les paquetages:

pty	FreeBSD-SA-08:01
libc	FreeBSD-SA-08:02

http://www.freebsd.org/security/index.html#adv

HP

Publication du document HPSBGN02301 (SSRT071508)

HP a publié le document HPSBGN02301 (SSRT071508) concernant une faille dans le contrôle ActiveX 'RulesEngine.dll'. Cette faille peut être exploitée à distance afin d'exécuter du code arbitraire ou d'obtenir des droits privilégiés sur une plate-forme Windows vulnérable. Cette faille affecte le produit 'Software Update' version 4.000.005.007 ou inférieure. Un correctif est disponible.

http://www11.itrc.hp.com/service/cki/docDisplay.do?docId=emr_na-c01311918-2&admit=109447626+1199780558667+28353475

CVE-2007-6506

Publication du document HPSBUX02303 (SSRT071468)

HP a publié le document HPSBUX02303 (SSRT071468) concernant la disponibilité de correctifs pour 'HP-UX'. Ils corrigent deux failles qui affectent le composant 'xfs' ('X Font Server') du serveur X Window 'X.Org' et permettent de provoquer l'exécution de code arbitraire avec les droits associés à 'xfs'.

http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01323725

CVE-2007-4990

Révision du bulletin HPSBMA02133 (SSRT061201)

HP a révisé le bulletin HPSBMA02133 (SSRT061201) concernant la vulnérabilité de HP 'Oracle for OpenView' à de nombreuses failles Oracle. Cette révision intègre les failles discutées dans le bulletin Oracle de Janvier 2008. HP recommande l'application des correctifs Oracle.

http://www11.itrc.hp.com/service/cki/docDisplay.do?docId=c00727143

IBM

Correctifs pour la faille CVE-2007-4474

IBM a publié le document 1279071 concernant la vulnérabilité référencée CVE-2007-4474, affectant les produits 'Lotus Domino Web Access'. Des débordements de buffer dans plusieurs contrôles ActiveX fournis avec ces produits permettent d'exécuter du code arbitraire. Les versions 6.5.6, 7.0.4 et 8.0.1 corrigent ces failles.

http://www-1.ibm.com/support/docview.wss?rs=463&uid=swg21279071

CVE-2007-4474

"Cross-Site Scripting" dans IBM ('Apache')

Une faille dans le produit 'Apache' affecte le produit IBM 'Websphere Application Server' pour 'z/OS'. Cette faille permet à un attaquant de mener des attaques de type "Cross-Site Scripting". Cette faille est similaire à celle précédemment discutée pour 'Apache'.

http://secunia.com/advisories/28375/

CVE-2007-5000

LINUX DEBIAN

Disponibilité de nombreux correctifs

Debian annonce la disponibilité des correctifs corrigeant les vulnérabilités présentes dans les paquetages:

tar	DSA-1438	type3-src	DSA-1439	inotify-tools	DSA-1440
peercast	DSA-1441	libsndfile	DSA-1442	tcpreen	DSA-1443
php5	DSA-1444	maradns	DSA-1445	wireshark	DSA-1446
tomcat5.5	DSA-1447	eggdrop	DSA-1448	lopp-aes-util	DSA-1449
util-linux	DSA-1450	mysql-dfsg	DSA-1451	wzdftp	DSA-1452
tomcat5	DSA-1453	freetype	DSA-1454	libarchive	DSA-1455
fail2ban	DSA-1456	dovecot	DSA-1457	openafs	DSA-1458
gforge	DSA-1459	postgresql8	DSA-1460	libxml2	DSA-1461
hplip	DSA-1462	postgresql7	DSA-1453	syslog-ng	DSA-1464
apt-listchanges	DSA-1465	xorg-server	DSA-1466	mantis	DSA-1467
tomcat5.5	DSA-1468	flac	DSA-1469	horde	DSA-1470
lib-vorbis	DSA-1471	xine-lib	DSA-1472	scponly	DSA-1473
exiv2	DSA-1474	gforge	DSA-1475	pulseaudio	DSA-1476
yarssr	DSA-1477	mysql-dfsg	DSA-1478	linux2.6	DSA-1479

http://www.debian.org/security/2008/

LINUX FEDORA

Disponibilité de nombreux correctifs

Fedora annonce la disponibilité des correctifs corrigeant les vulnérabilités présentes dans les paquetages:

gallery2	F7	FEDORA-2007:4777	F8	FEDORA-2007:4778
imlib	F7	FEDORA-2007:4561	F8	FEDORA-2007:4594
qt4	F7	FEDORA-2007:4354	F8	FEDORA-2007:4285
wordpress	F7	FEDORA-2008:0126	F8	FEDORA-2008:0103

libcdio	F7	FEDORA-2008:0104	F8	FEDORA-2008:0136
asterisk	F7	FEDORA-2008:0198	F8	FEDORA-2008:0199
mantis	F7	FEDORA-2008:0282	F8	FEDORA-2008:0353
python-cherry	F7	FEDORA-2008:0333	F8	FEDORA-2008:0289
libxml2	F7	FEDORA-2008:0477	F8	FEDORA-2008:0462
qimageblitz	F7	FEDORA-2008:0462	F8	FEDORA-2008:0536
drupal	F7	FEDORA-2008:0469	F8	FEDORA-2008:0485
tog-pegasus	F7	FEDORA-2008:0506	F8	FEDORA-2008:0572
postgresql8	F7	FEDORA-2008:0552	F8	FEDORA-2008:0478
moodle	F7	FEDORA-2008:0627	F8	FEDORA-2008:0610
python-paramiko	F7	FEDORA-2008:0722	F8	FEDORA-2008:0644
xine-lib			F8	FEDORA-2008:0718
syslog-ng	F7	FEDORA-2008:0559	F8	FEDORA-2008:0523
e2fsprog	F7	FEDORA-2007:4461	F8	FEDORA-2007:4447
cairo	F7	FEDORA-2007:3818		
xorg-x11	F7	FEDORA-2008:0831	F8	FEDORA-2008:0760
clamav	F7	FEDORA-2008:0170	F8	FEDORA-2008:0115
mantis	F7	FEDORA-2008:0796	F8	FEDORA-2008:0856
libXfont	F7	FEDORA-2008:0891	F8	FEDORA-2008:0794
hsqldb	F7	FEDORA-2008:4119	F8	FEDORA-2007:4171
boost	F7	FEDORA-2008:0880		
bind	F7	FEDORA-2008:0904	F8	FEDORA-2008:0903
xorg-x11	F7	FEDORA-2008:0956	F8	FEDORA-2008:0930
kernel2.6			F8	FEDORA-2008:0748
pulseaudio	F7	FEDORA-2008:0994	F8	FEDORA-2008:0963
icu	F7	FEDORA-2008:1076	F8	FEDORA-2008:1036
xine-lib	F7	FEDORA-2008:1047	F8	FEDORA-2008:1043
kernel2.6	F7	FEDORA-2008:0958		

https://www.redhat.com/archives/fedora-package-announce/index.html

LINUX MANDRIVA

Disponibilité de nombreux correctifs

Mandrake annonce la disponibilité des correctifs corrigeant les vulnérabilités présentes dans les paquetages:

wireshark	MDVSA-2008:001	2007.0	2007.1	2008		CS4.0	
squid	MDVSA-2008:002	2007.0	2007.1	2008	CS3.0	CS4.0	MNF2.0
clamav	MDVSA-2008:003	2007.0	2007.1	2008	CS3.0	CS4.0	
postgresql	MDVSA-2008:004	2007.0	2007.1	2008	CS3.0	CS4.0	
libexif	MDVSA-2008:005		2007.1	2008			
exiv2	MDVSA-2008:006	2007.0	2007.1	2008	CS3.0	CS4.0	MNF2.0
madwifi-source	MDVSA-2008:007	2007.0	2007.1	2008			
kernel	MDVSA-2008:008					CS4.0	
autofs	MDVSA-2008:009	2007.0	2007.1	2008			
libxml2	MDVSA-2008:010	2007.0	2007.1	2008	CS3.0	CS4.0	
rsync	MDVSA-2008:011	2007.0	2007.1	2008	CS3.0	CS4.0	
python	MDVSA-2008:012				CS3.0		MNF2.0
python	MDVSA-2008:013	2007.0	2007.1	2008		CS4.0	
apache1	MDVSA-2008:014				CS3.0		
apache2	MDVSA-2008:015				CS3.0		MNF2.0
apache2	MDVSA-2008:016	2007.0	2007.1	2008		CS4.0	
mysql	MDVSA-2008:017			2008			
gftp	MDVSA-2008:018		2007.1				
cairo	MDVSA-2008:019	2007.0	2007.1	2008		CS4.0	
xine-lib	MDVSA-2008:020		2007.1	2008			
xfree86	MDVSA-2008:021				CS3.0		
xorg-x11	MDVSA-2008:022					CS4.0	
x11-server	MDVSA-2008:023	2007.0	2007.1	2008			
libxfont	MDVSA-2008:024	2007.0	2007.1	2008			
x11-server-xgl	MDVSA-2008:025	2007.0	2007.1	2008			
icu	MDVSA-2008:026			2008			
pulseaudio	MDVSA-2008:027		2007.1	2008			
mysql	MDVSA-2008:028	2007.0	2007.1			CS4.0	

http://www.mandriva.com/en/security/advisories

LINUX REDHAT

Disponibilité de nombreux correctifs

RedHat annonce la disponibilité des correctifs corrigeant les vulnérabilités présentes dans les paquetages:

top-pegasus	RHSA-2008:0002-01			AS.ES.WS 4.0	AS.ES.WS 5.0
e2fsprogs	RHSA-2008:0003-01	AS.ES.WS 2.1	AS.ES.WS 3.0	AS.ES.WS 4.0	AS.ES.WS 5.0
libxml2	RHSA-2008:0032-01	AS.ES.WS 2.1	AS.ES.WS 3.0	AS.ES.WS 4.0	AS.ES.WS 5.0
postgresql	RHSA-2008:0038-01			AS.ES.WS 4.0	AS.ES.WS 5.0
postgresql	RHSA-2008:0039-01		AS.ES.WS 3.0		

apache	RHSA-2008:0004-01	AS.ES.WS 2.1			
httpd	RHSA-2008:0005-01		AS.ES.WS 3.0		
httpd	RHSA-2008:0006-01			AS.ES.WS 4.0	
httpd	RHSA-2008:0007-01			AS.ES.WS 4.0	
httpd	RHSA-2008:0008-01				AS.ES.WS 5.0
xorg-x11	RHSA-2008:0030-01			AS.ES.WS 4.0	
xorg-x11	RHSA-2008:0031-01				AS.ES.WS 5.0
lib-xfont	RHSA-2008:0064-01				AS.ES.WS 5.0
xfree86	RHSA-2008:0029-01	AS.ES.WS 2.1	AS.ES.WS 3.0		
wireshark	RHSA-2008:0058-01			AS.ES.WS 4.0	AS.ES.WS 5.0
wireshark	RHSA-2008:0059-01		AS.ES.WS 3.0		
httpd	RHSA-2008:0009-01				AS.ES.WS 5.0
kernel	RHSA-2008:0089-01				AS.ES.WS 5.0
icu	RHSA-2008:0090-01				AS.ES.WS 5.0

https://www.redhat.com/archives/enterprise-watch-list/

LINUX SuSE

Disponibilité de nombreux correctifs

SuSE annonce la disponibilité des correctifs corrigeant les vulnérabilités présentes dans les paquetages:

flash-player	SUSE-SA:2007:069	opera	SUSE-SA:2008:001
xorg	SUSE-SA:2008:002		
Summary Report 26	SR_2007_26	Summary Report 01	SR_2008_01
Summary Annonce 01	SA_2008_02	Summary Report 02	SR_2008_02

http://www.novell.com/linux/security/advisories.html

MICROSOFT

Révision du bulletin Microsoft MS08-001 (941644)

Microsoft a révisé le bulletin MS08-001 (941644) concernant deux failles dans la pile 'TCP/IP' des plate-formes Windows qui permettent de provoquer des dénis de service et l'exécution de code arbitraire. Cette révision annonce l'ajout de la plate-forme 'Windows Small Business Server 2003' version SP2 dans la liste des produits vulnérables. Un correctif est également disponible.

http://www.microsoft.com/technet/security/Bulletin/MS08-001.mspx

CVE-2007-0066, CVE-2007-0069

Révision du bulletin Microsoft MS08-001 (941644)

Microsoft a révisé le bulletin MS08-001 (941644) concernant deux failles dans la pile 'TCP/IP' des plate-formes Windows qui permettent de provoquer des dénis de service et l'exécution de code arbitraire. Cette révision met à jour les informations concernant la faille référencée CVE-2007-0069 pour les plate-formes 'Windows Small Business Server 2003' et 'Windows Home Server'.

http://www.microsoft.com/technet/security/Bulletin/MS08-001.mspx

CVE-2007-0066, CVE-2007-0069

SUN

Correctifs pour la faille 'FreeType' CVE-2007-2754

Sun a annoncé, dans le bulletin 103171, la vulnérabilité de la bibliothèque 'FreeType' fournie avec 'Solaris' versions 8, 9 et 10 à la faille référencée CVE-2007-2754. Elle permet d'exécuter du code arbitraire. Des correctifs sont disponibles.

http://sunsolve.sun.com/search/document.do?assetkey=1-26-103171-1

CVE-2007-2754

Publication du document 103197

Sun a publié le document 103197 concernant de multiples failles dans la base de données 'PostgreSQL' qui permettent de provoquer un déni de service d'un serveur ou autorisent un utilisateur malveillant à obtenir des droits privilégiés.

http://sunsolve.sun.com/search/document.do?assetkey=1-26-103197-1

CVE-2007-3278, CVE-2007-4769, CVE-2007-4772, CVE-2007-6067, CVE-2007-6600, CVE-2007-6601

Publication du document 103201

Sun a publié le document 103201 concernant une faille non documentée dans la bibliothèque 'Libxml2' qui permet à un attaquant de provoquer un déni de service.

http://sunsolve.sun.com/search/document.do?assetkey=1-26-103201-1

CVE-2007-6284

Révision du bulletin 103069

Sun a révisé le bulletin 103069 concernant des failles non documentées dans le produit 'Sun Java System Access Manager' qui permettent d'obtenir un accès non autorisé et de provoquer l'exécution de code arbitraire avec des droits privilégiés. Cette révision annonce la mise à jour les sections "Contributing Factors" et "Resolution".

http://sunsolve.sun.com/search/document.do?assetkey=1-26-103069-1

Révision du bulletin 103069

Sun a révisé le bulletin 103069 concernant des failles non documentées dans le produit 'Sun Java System Access Manager' qui permettent d'obtenir un accès non autorisé et de provoquer l'exécution de code arbitraire avec des droits privilégiés. Cette révision annonce la mise à jour des sections "Contributing Factors" et "Resolution".

http://sunsolve.sun.com/search/document.do?assetkey=1-26-103069-1

Révision du bulletin 103114

Sun a révisé le bulletin 103114 concernant la vulnérabilité du composant 'xfs' fourni avec 'Solaris' versions 8, 9 et 10 aux failles référencées CVE-2007-4568 et CVE-2007-4990. Ces failles permettent d'exécuter du code arbitraire. Cette révision annonce la mise à jour des sections "Contributing Factors" et "Resolution", et clos le bulletin.

http://sunsolve.sun.com/search/document.do?assetkey=1-26-103114-1

CVE-2007-4568, CVE-2007-4990

Révision du bulletin 103162

Sun a révisé le bulletin 103162 concernant une faille dans Sun 'Solaris 10' qui permet à un attaquant de contourner la sécurité et d'obtenir les privilèges "root". Cette révision annonce la mise à jour de la section "Impact".

http://sunsolve.sun.com/search/document.do?assetkey=1-26-103162-1

Révision du bulletin 103177

Sun a révisé le bulletin 103177 concernant la vulnérabilité des produits 'Firefox' et 'Thunderbird' fournis avec 'Solaris' version 10 aux failles MFSA 2007-18 à MFSA 2007-27. Cette révision met à jour les sections "Updated Impact", "Contributing Factors", "Relief/Workaround" et "Resolution".

http://sunsolve.sun.com/search/document.do?assetkey=1-26-103177-1

CVE-2007-3089, CVE-2007-3285, CVE-2007-3656, CVE-2007-3734, CVE-2007-3735, CVE-2007-3736, CVE-2007-3737, CVE-2007-3738, CVE-2007-3844, CVE-2007-3845

Révision du bulletin 103180

Sun a révisé le bulletin 103180 concernant de multiples failles non documentées dans le produit Sun 'Java System Identity Manager' qui permettent de mener de attaques de type "Cross-Site Scripting". Cette révision annonce la mise à jour les sections "Contributing Factors" et "Resolution".

http://sunsolve.sun.com/search/document.do?assetkey=1-26-103180-1

Révision du bulletin Sun 103150

Sun a révisé le bulletin 103150 concernant la vulnérabilité de l'outil 'unzip' de 'Solaris' à la faille référencée CVE-2005-0602, qui permet à un utilisateur local d'élever ses privilèges. Cette révision annonce la mise à jour des sections "Contributing Factors" et "Resolution", et clos le bulletin.

http://sunsolve.sun.com/search/document.do?assetkey=1-26-103150-1

CVE-2005-0602

VMWARE

Correctifs pour les produits VMware

VMware a annoncé, dans le document VMSA-2008-0002, la disponibilité de correctifs pour les produits 'VirtualCenter Management Server' version 2, et 'ESX Server' versions 3.0.1 et 3.0.2. Ils corrigent des failles dans les produits 'Tomcat' et 'Java'.

http://lists.grok.org.uk/pipermail/full-disclosure/2008-January/059478.html

CVE-2005-2090, CVE-2006-7195, CVE-2007-0450, CVE-2007-3004

Correctifs pour les produits VMware

VMware a annoncé, dans le document VMSA-2008-0001, la disponibilité de correctifs pour les produits 'ESX Server' versions 3.0.1 et 3.0.2. Ils corrigent de multiples failles dans les produits 'OpenPegasus', 'Samba', 'Perl' et 'OpenSSL'.

http://lists.grok.org.uk/pipermail/full-disclosure/2008-January/059479.html

CVE-2007-3108, CVE-2007-4572, CVE-2007-5116, CVE-2007-5135, CVE-2007-5191, CVE-2007-5360, CVE-2007-5398

XEROX

Failles 'samba' dans 'ESS/Network Controller'

Xerox a publié le document XRX08-001 concernant la vulnérabilité des produits 'ESS/Network Controller' aux failles 'samba' référencées CVE-2007-2446 et CVE-2007-2447. Elles permettent l'exécution de code et de commandes arbitraires. Le correctif P32 est disponible auprès du support Xerox.

http://www.xerox.com/downloads/usa/en/c/cert_XRX08_001.pdf

CVE-2007-2446, CVE-2007-2447

US-CERT

Reprise de l'alerte Oracle de Janvier 2008

L'US-CERT a repris, sous la référence TA08-017A concernant de multiples vulnérabilités dans les produits Oracle qui peuvent entraîner de nombreuses conséquences.

http://www.us-cert.gov/cas/techalerts/TA08-017A.html

Reprise des alertes Apple sur 'QuickTime'

L'US-CERT a repris, sous la référence TA08-016A les alertes Apple sur 'QuickTime' concernant de multiples failles dans 'QuickTime' qui permettent à un attaquant d'exécuter du code arbitraire et de provoquer un déni de service.

http://www.us-cert.gov/cas/techalerts/TA08-016A.html

CVE-2008-0031, CVE-2008-0032, CVE-2008-0033, CVE-2008-0036

Reprise des bulletins Microsoft de janvier 2008
L'US-CERT a repris, sous la référence TA08-008A, les bulletins Microsoft de janvier 2008 concernant des failles dans les plate-formes Windows qui permettent d'obtenir des droits privilégiés, d'exécuter du code arbitraire et de provoquer des dénis de service.
http://www.uscert.gov/cas/techalerts/TA08-008A.html
CVE-2007-0066, CVE-2007-0069, CVE-2007-5352

CODES D'EXPLOITATION

Les codes d'exploitation des vulnérabilités suivantes ont fait l'objet d'une large diffusion :

IBM

Codes d'exploitation pour la faille CVE-2007-4474
Deux code ont été publiés sur la liste de diffusion Full Disclosure. Ils exploitent la faille IBM référencée CVE-2007-4474, dans un contrôle ActiveX de 'Lotus Domino Web Access'. Ces codes malicieux permettent d'exécuter la calculatrice Windows sur une plate-forme vulnérable.
http://lists.grok.org.uk/pipermail/full-disclosure/2007-December/059365.html
http://lists.grok.org.uk/pipermail/full-disclosure/2007-December/059368.html
CVE-2007-4474

MICROSOFT

Code d'exploitation pour la faille CVE-2007-3901
Un code a été publié sur le site Web Milw0rm exploitant la faille Microsoft référencée CVE-2007-3901, permettant d'exécuter du code arbitraire à l'aide d'un fichier 'SAMI' spécialement construit. Ce code sert un fichier 'SAMI' malicieux qui permet d'obtenir un interpréteur de commandes à distance sur le port TCP/4444 lorsqu'il sera ouvert par une machine vulnérable.
http://milw0rm.com/exploits/4866
CVE-2007-3901

BULLETINS ET NOTES

Les bulletins d'information suivants ont été publiés par les organismes officiels de surveillance et les éditeurs :

VIRUS

Apparition du ver 'Beselo'
L'US-CERT, ainsi que F-Secure, nous informent de l'apparition d'un code malicieux visant les plate-formes mobiles Symbian. Ce code, nommé 'Beselo', se diffuse via Bluetooth et des messages MMS. Il utilise des techniques d'ingénierie sociale afin de s'installer. Il est fortement recommandé de mettre à jour vos signatures antivirus pour votre appareil mobile.
http://www.f-secure.com/weblog/archives/00001368.html
http://www.uscert.gov/current/index.html#symbianos_worm

ATTAQUES

OUTILS

ERRATASEC – FERRET V1.1

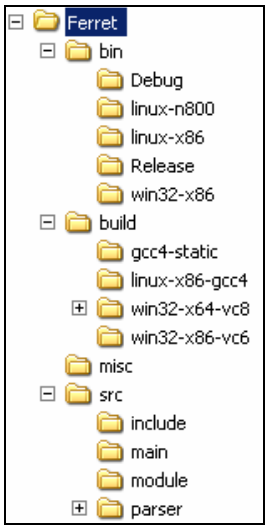
- **Description**

En février 2007 et à l'occasion de la conférence **BlackHat 2007**, **David Maynor** et **Robert Graham** intervenants connus dans le monde de la sécurité et fondateurs de la société **ErrataSecurity** proposaient au téléchargement l'utilitaire '**Ferret**' dans le cadre de leur intervention intitulée '**How to Give Attackers a Roadmap to Your Network**' (Rapport N°104 – Mars 2007).

L'idée originale ayant conduit à l'écriture de cet utilitaire est que les protocoles de communication divulguent un très grand nombre d'informations sur leurs utilisateurs sans que ces derniers n'en soient toujours conscients. Rien qui ne soit réellement innovant – le data mining existe de longue date et nombreux sont ceux qui savent tirer parti des données contenues dans les protocoles – mais les auteurs décrivaient une approche allant au-delà de la simple collecte et utilisation immédiate des données acquises à des fins d'attaque du système pour se rapprocher de procédés en usage dans les métiers du renseignement. Au point d'ailleurs de souffrir des mêmes maux: la complexité à corréler une grande quantité d'informations hétérogènes et éparses.

Les auteurs nous mettaient l'eau à la bouche en nous présentant un agrégateur de données devant permettre d'y voir un peu clair dans la multitude d'informations acquises par leur utilitaire de collecte, le susnommé '**Ferret**'. Hélas, si une nouvelle version de ce dernier vient de voir le jour, qui corrige différents bogues de programmation et intègre quelques nouvelles fonctionnalités, les auteurs annoncent qu'ils ne sont toujours pas prêt à diffuser '**Ferret Viewer**' leur outil d'agrégation:

> *'we aren't ready to release the "viewer" utility that correlates it, although it's fairly straight forward to parse the command-line output and do your own correlation'.*



Quoiqu'il en soit, les corrections et fonctionnalités apportées à cette nouvelle version en font un outil désormais intéressant contrairement à la version originale dont nous disions lors de son test qu'elle «*était plus proche du démonstrateur que de l'outil réellement exploitable*».

Tout d'abord, la distribution a été réorganisée pour faciliter la compilation dans les différents environnements cibles: Linux et Windows avec désormais le support du compilateur **VC8.0**. L'utilisateur trouvera tous les fichiers requis dans les sous répertoires du répertoire 'build'. Les tests menés en environnement Windows et Linux n'ont mis en évidence aucun problème, ni de compilation, ni d'exécution.

Les auteurs ont ensuite documenté toute l'architecture de leur programme, les choix d'implémentation et les astuces de codage dans le fichier texte '**read-code**' présent à la racine de la distribution. On pourra d'ailleurs ne pas toujours être en accord avec certains des principes exposés dont celui consistant à ne pas laisser au compilateur le choix des optimisations, ou encore d'affecter la variable représentative de l'état d'un automate dans le corps de la fonction '**printf()**', une approche qui conduira à coup sûr à une erreur lors de la modification du code. L'approche retenue pour le réassemblage des données est par contre très intéressante.

Après compilation, l'utilitaire pourra être lancé à condition toutefois que la librairie '**libpcap**' en environnement LINUX, ou son pendant '**WinpCap**' en environnement Windows, ait été installée.

La sélection du périphérique réseau à partir duquel seront acquises les données est facilité par l'affichage des périphériques disponibles et de leur numéro de référence que l'on utilisera conjointement avec l'option '**-i**'.

L'option '**-c**' permet de spécifier un fichier de configuration dans lequel seront définis tous les paramètres spécifiques et en particulier le répertoire qui contiendra les données acquises au format '**pcap**'.

Au regard des protocoles réseaux et applicatifs pour lesquels un analyseur a été écrit, la question se pose de savoir s'il n'aurait pas été plus intéressant de s'appuyer sur une plate-forme dédiée à l'analyse réseau. Nous pensons notamment à **WireShark** lequel intègre de très nombreux protocoles et dont les modules d'analyse – dissecteurs dans le jargon – peuvent aisément être adaptés au besoin ici exprimé.

PILES	STREAM	PARSERS
ARP	*AIM*	*DNS*
Apple Talk	*HTTP*	*ISAKKMP*
Ethernet	*MSN*	*JPEG*
GRE	*POP3*	*LDAP*
ICMP	*SMTP*	*NETBIOS*
IEEE 802.1X	**PARSERS**	*PPP*
IGMP	*Apple Talk*	*SIP*
IPv4 et IPv6	*BitTorrent*	*SMB*
IPX	*CallWave IM*	*SNMP*
TCP	*CISCO*	*SRVLOC*
UDP	*CUPS*	*UPnP SSDP*
IEEE 802.11	*DHCP*	*TiVO*

- **Complément d'information**

http://www.erratasec.com/ferret.html
https://www.blackhat.com/presentations/bh-dc-07/Maynor_Graham/Presentation/bh-dc-07-Maynor_Graham-up.pdf