APOGEE Communications

Rapport de
Veille Technologique Sécurité
N°110

Septembre 2007

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 …

Notre rapport de Septembre sera très succinct car notre lecteur l'aura peut être remarqué, notre adresse postale a changé. Notre activité vient en effet de rejoindre ses nouveaux locaux sis à **Massy-Palaiseau** occasionnant une surcharge de travail ponctuelle ne nous ayant pas permis d'assurer autant qu'à l'accoutumé notre activité.

Nos adresses de courrier électronique restent inchangées mais nous disposons désormais d'un numéro de téléphone dédié à notre activité de veille et de gestion d'incidents, le 01.69.85.78.90

Nous sommes par ailleurs heureux de vous informer que notre équipe est désormais référencée sur la liste des **CSIRT** Européens gérée par l'opérateur **S-Cure** dans le cadre du projet **TI** '**Trusted Introducer**'.

http://www.trusted-introducer.nl/teams/teams-a.html#APOGEE-SECWATCH

En attendant notre prochain rapport, nos lecteurs pourront s'occuper avec la lecture des quelques 75 présentations de la dernière édition de **BlackHat**.

http://www.blackhat.com/html/bh-media-archives/bh-archives-2007.html

Bertrand VELLE

PRODUITS ET TECHNOLOGIES

LES PRODUITS

DECOMPILATION

HEX-RAYS

- **Description**

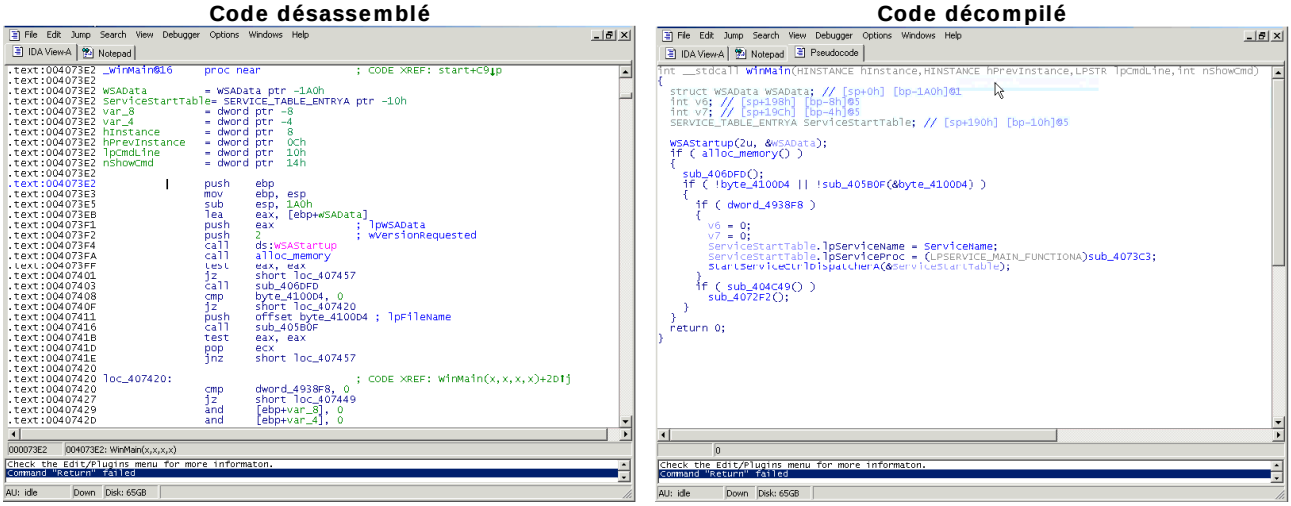
Hex-Rays Au début des années 90, un logiciel révolutionnait la petite communauté des bidouilleurs – nous préférons ce terme à celui de hackers – en offrant une fonctionnalité n'existant alors que dans l'imagination des développeurs: la désassemblage d'un code binaire dans une représentation bien plus facile à appréhender que le code assembleur du processeur bien que l'on ne puisse encore réellement parler de 'décompilation'. Dénommé '**The Sourcer**', ce logiciel rejoignait rapidement la boîte à outils de développeurs et plus largement de la communauté des passionnés.

Au milieu des années 90, un certain **Ilfak Guilfanov** postait dans un news group la description d'une approche permettant de simplifier l'analyse d'un code binaire en identifiant automatiquement les portions de ce code correspondant à des fonctions appartenant aux bibliothèques de base du système. Utilisant un mécanisme de signatures, cette approche était mise en pratique dans un outil dénommé '**I**nteractive **D**is**A**ssembler' ou **IDA** dont une première version était publiée courant 95. L'on sait le succès qu'a connu, et que connaît encore, cet outil distribué par la société '**Datarescue**'.

Le même **Ilfak Guilfanov** vient de fonder la société '**Hex-Rays**' domiciliée en Belgique tout comme **DataRescue**. Cette nouvelle société est chargée de l'édition et de la distribution d'un nouvel outil venant en complément de la dernière version de l'outil **IDA-Pro**. Cet outil dénommé '**Hex-Rays Decompiler**' est annoncé pouvoir générer une représentation de n'importe quel exécutable Intel x86 32bits dans un pseudo-code proche du langage 'C' en quelques secondes seulement.

Aucune version de démonstration de cet outil - vendu $1999 ou €1500 auquel il faut rajouter le prix de la licence de la version 5.1 d'IDA-Pro soit $470 ou €360 en version de base - n'est hélas disponible. Seule une vidéo proposée sur le site de la société permet de se rendre compte de son incroyable efficacité.

Code désassemblé **Code décompilé**



Extrait de la vidéo proposée sur le site Hex-Rays

Nos lecteurs intéressés, ou simplement intrigués, par les performances de cet outil pourront étudier différents exemples de décompilation proposés sur une page du site laquelle met en vis-à-vis la version désassemblée à l'aide d'IDA et la version décompilée à l'aide d'Hex-Rays..

- **Complément d'information**

http://www.hex-rays.com/	- Hex-Rays
http://www.hex-rays.com/compare.shtml	- Comparaison des approches
http://www.datarescue.com/idabase/index.htm	- IDA pro via Datarescue
http://www.idapro.ru/	- IDA pro

INFORMATIONS ET LEGISLATION

LES INFORMATIONS

CONFERENCES

BLACKHAT USA 2007

- **Description**

L'édition américaine de la conférence **BlackHat**, suivie de la conférence **DefCon**, s'est tenue du 28 juillet au 2 août à Las Vegas. Les supports de la majorité des 86 présentations – 79 pour l'édition 2006 – sont désormais disponibles en ligne.

Nous proposons ci-dessous une liste des présentations par nous triées par thèmes:

Analyse	
Anonymity and its Discontents	L.Sassaman
Blackout: What Really Happened...	J.Butler & K.Kendall
Disclosure and Intellectual Property Law: Case Studies	J.Granick
Don't Tell Joanna, The Virtualized Rootkit Is Dead	T.Ptacek & N.Lawson
Estonia: Information Warfare and Strategic Lessons	G.Evron
Greetz from Room 101	K.Geers
IsGameOver(), anyone?	J.Rutkowska & all
It's All About the Timing	H.Meer & M.Slaviero
Kick Ass Hypervisoring: Windows Server Virtualization (part1 / part 2)	B.Baker
Longhorn Server Foundation & Server Roles	I.McDonald
RFID for Beginners++	C.Paget
Smoke 'em Out!	R.Belani & K.Jones
Social Network Site Data Mining	S.Patton
Strengths and Weaknesses of Access Control Systems	E.Schmiedl & all
Tactical Exploitation	HD Moore & Valsmith
Tor and Blocking-resistance	R.Dingledine
Unforgivable Vulnerabilities	S.Christey
Vista Network Attack Surface Analysis and Teredo Security Implications	J.Hoagland
Détection	
CaffeineMonkey: Automated Collection, Detection, Analysis of Malicious JavaScript	B.Feinstein & D.Peck
PISA: Protocol Identification via Statistical Analysis	R.Dhamankar & R.King
Sphinx: An Anomaly-based Web Intrusion Detection System	D.Bolzoni & E.Zambon
Traffic Analysis—The Most Powerful and Least Understood Attack Methods	J.Callas & all
Forensique	
A Picture's Worth...	Dr. Neal Krawetz
Active Reversing: The Next Generation of Reverse Engineering	G.Hoglund
Breaking Forensics Software: Weaknesses in Critical Evidence Collection	C.Palmer & all
Database Forensics	D.Litchfield
Iron Chef Blackhat (part 1 / part 2)	B.Chess & all
PyEmu: A multi-purpose scriptable x86 emulator	C.Pierce
Reverse Engineering Automation with Python	Ero Carrera
Reversing MSRC Updates: Case Studies of MSRC Bulletins 2004–2007	G.Wroblewski
SQL Server Database Forensics	K.Fowler
Static Detection of Application Backdoors	C.Wysopal & C.Eng
The Art of Unpacking	MV.Yason
Hacking	
(un)Smashing the Stack	S.Moyer
Attacking the Windows Kernel	J.Lindsay
Attacking Web Service Security	B.Hill
Black Ops 2007: Design Reviewing The Web	D.Kaminksy
Breaking C++ Applications	M.Dowd & all
Building and Breaking the Browser	W.Snyder & M.Shaver
Covert Debugging: Circumventing Software Armoring Techniques	D.Quist & Valsmith
Dangling Pointer	Jonathan Afek
Exposing Vulnerabilities in Media Software	D.Thiel

Fuzzing Sucks! (or Fuzz it Like you Mean it!)	P.Amini & A.Portnoy
Hacking Capitalism	B.D.G., & J.Rauch
Hacking Intranet Websites from the Outside	J.Grossman & R.Hansen
Hacking Leopard: Tools and techniques for attacking the newest Mac OS X	C.Miller
Hacking the Extensible Firmware Interface	J.Heasman
Heap Feng Shui in JavaScript	A.Sotirov
Injecting RDS-TMC Traffic Information Signals	A.Barisani & D.Bianco
Intranet Invasion With Anti-DNS Pinning	D.Byrne
Just Another Windows Kernel Perl Hacker	J.Stewart
Kernel Wars	J.Eriksson & all
NACATTACK	DJ.Roecher & all
OpenBSD Remote Exploit	A.Ortega
Other Wireless: New ways of being Pwned	L.Miras
Point, Click, RTPInject	Z.Lackey & A.Garbutt
Premature Ajax-ulation	B.Sullivan & B.Hoffman
Reflection DNS Poisoning	J.Schneider
Remote and Local Exploitation of Network Drivers	Y.Bulygin
Reversing C++	PV.Sabanal
Revolutionizing the Field of Grey-box Attack Surface Testing	J.DeMott & all
RFIDIOts!!!– Practical RFID Hacking	A.Laurie
Side Channel Attacks (DPA) and Countermeasures for Embedded Systems	Job De Haas
Something Old (H.323), Something New (IAX), ...	H.Dwivedi & Z.Lackey
Stealth Secrets of the Malware Ninjas	N.Harbour
Timing Attacks for Recovering Private Entries From Database Engines	A.Waissbein & D.Saura
Type Conversion Errors: How a Little Data Type Can Do a Whole Lot of Damage	J.Morin
Understanding the Heap by Breaking It	J.N. Ferguson
Malware et Virus	
Observing the Tidal Waves of Malware	S.Zanero
Status of Cell Phone Malware in 2007	M.Hypponen
The Little Hybrid Web Worm that Could	B.Hoffman & J.Terrill
Prévention	
A Dynamic Technique for Enhancing the Security and Privacy of Web Applications	ED.Gutesman & all
Anonymous Authentication— Preserving Your Privacy Online	Dr. Andrew Lindell
Blind Security Testing—An Evolutionary Approach	S.Stender
Building an Effective Application Security Practice	RW.Clark
Defeating Information Leak Prevention	E.Monti & D.Moniz
Defeating Web Browser Heap Spray Attacks	S.Chenette & all
OpenID: Single Sign-On for the Internet	E.Tsyrklevich & all
Practical Sandboxing - Techniques for Isolating Processes	D.LeBlanc
Securing the Tor Network	M.Perry
Simple Solutions to Complex Problems from the Lazy Hacker's Handbook	D.Maynor & R.Graham
The Security Analytics Project: Alternatives in Analysis	M.Ryan
VoIP	
Transparent Weaknesses in VoIP	P.Thermos
VoIP Security: Methodology and Results	B.Dempster
Vulnerabilities in Wi-Fi/Dual-Mode VoIP Phones	K.Kurapati
Z-Phone	P.Zimmermann

- **Complément d'information**

http://www.blackhat.com/html/bh-media-archives/bh-archives-2007.html

METHODES

OCTAVE - ALLEGRO

- **Description**

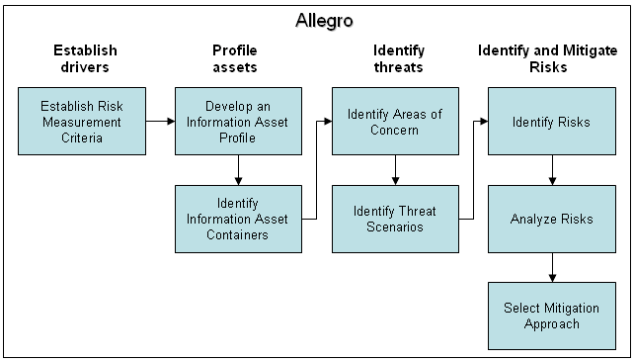
La méthodologie d'évaluation des risques **Octave** (**O**perationally **C**ritical **T**hreat, **A**sset, and **V**ulnerability **E**valuation) a été développée en 1999 par l'université de **Carnegie Mellon** (**CMU**) puis régulièrement améliorée jusqu'en juin 2003 où le guide de mise en œuvre '**OCTAVE Method Implementation Guide**' était publié dans sa seconde édition (Rapport N°59 – Juin 2003).

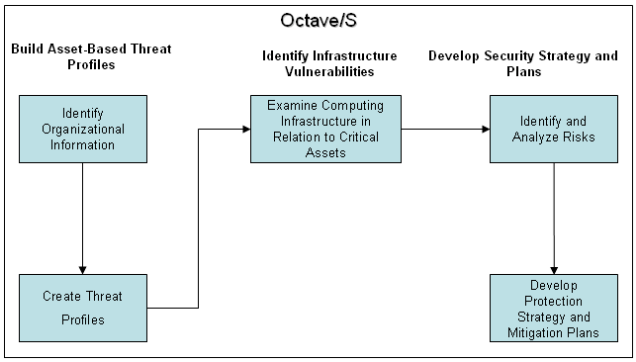
En septembre 2003, une adaptation de la méthode dénommée **Octave/S** ('**S**' pour **Small**) était proposée pour répondre aux besoins spécifiques des petites structures – moins d'une centaine de personnes – en épurant la méthode de base de certaines actions dont les résultats sont supposés déjà être connus de l'équipe d'analyse constituée de 3 à 5 personnes (Rapport N°62 – Septembre 2003). Le guide de cette méthode est toujours disponible en version préliminaire, aucune mise à jour n'ayant été effectuée depuis la date de sa publication initiale.

Fin août dernier, une nouvelle méthode dénommée '**Allegro**' était annoncée sur le portail d'information dédié à la méthode **Octave**. Conçue pour répondre elle aussi aux besoins d'organisations de petite taille – une centaine de personnes – cette méthode n'est pas destinée à remplacer la méthode **Octave/S** mais à compléter celle-ci en se focalisant non plus sur l'évaluation des risques au sens large mais sur les risques liés aux actifs informationnels.

Le retour d'expérience sur l'application des différentes déclinaisons de l'approche **Octave** montre en effet qu'un recentrage de l'approche sur les actifs informationnels dans le contexte de leur utilisation au sein de l'organisation est devenu nécessaire. Il faut pour cela analyser les risques et menaces en tenant compte de l'utilisation qui est faite de ces informations, à leur stockage, à leur transport et aux traitements qui leur sont appliqués.

L'approche **Octave Allegro** prend en compte cette nouvelle dimension de l'analyse de risque en proposant une démarche qui se décline en huit étapes et qui peut être mise en œuvre par une petite équipe avec un minimum de moyens et sans nécessiter de recours à une expertise pointue comme cela est aussi le cas de la méthode **Octave/S**.





Cette méthode est documentée dans un rapport technique de 154 pages intitulé '**Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process**' et référencé '**CMU/SEI-2007-TR-012**'.

La table des matières est la suivante:

- **Complément d'information**

http://www.cert.org/octave/methods.html
http://www.cert.org/archive/pdf/07tr012.pdf

DCSSI – METHODOLOGIE GISSIP

- **Description**

Fin août, le portail de la **D**irection **C**entrale de la **S**écurité des **S**ystèmes d'**I**nformation (**DCSSI**) s'est enrichi d'un guide détaillant une approche destinée à faciliter l'intégration de la composante sécurité des systèmes d'information dans un projet en vue d'obtenir son homologation, c'est-à-dire la déclaration par une autorité que le système résultant « *est bien apte à protéger les informations qu'il doit traiter conformément aux besoins de sécurité exprimé et que les risques de sécurité résiduels sont acceptés et maîtrisés.*»

Dénommé '**G**uide d'**I**ntégration de la **S**écurité des **S**ystèmes d'**I**nformation dans les **P**rojets dit **GISSIP**, ce nouveau document de 49 pages a été réalisé par le bureau conseil de la **DCSSI**, la version publiée datant de décembre 2007.

Il propose une démarche pratique permettant d'identifier les actions devant être engagées, et les livrables devant être produits, tout au long du cycle de vie d'un système d'information en tenant compte d'un paramètre d'ajustement représentatif du niveau de maturité de l'organisation appliquant la méthodologie.

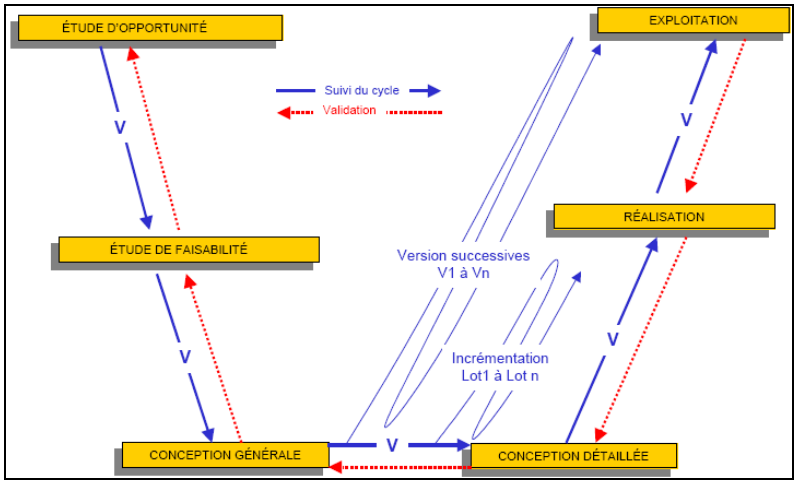
Cinq niveaux de maturité sont ainsi définis allant du **niveau 0** représentatif d'un contexte dans lequel la sécurité des systèmes d'information ou **SSI** n'est pas du tout prise en compte dans le cycle du vie du SI au **niveau 5** correspondant à une environnement dans lequel la SSI est bien intégrée au cycle de vie et en constante amélioration.

Sont aussi définis:

- **un cycle de vie** qui est représentatif de l'évolution d'une grande majorité de SI de la phase initiale de prise de décision à celle de l'exploitation. Prenant la forme d'un cycle en V, le modèle générique proposé et reproduit ci-contre pourra parfaitement être adapté au contexte.

  On remarquera cependant l'absence de la phase de fin de vie du système dite de 'disposition' ou de 'décommissionnement' pourtant prise en compte par d'autres cycles dont celui utilisé du **NIST**.

  Rappelons pour mémoire que ce dernier, défini notamment dans le guide **SP800-64** Rev.1 '**Security Considerations in the Information System Development Life Cycle**' comporte 5 phases:
  - Initialisation,
  - Acquisition et développement,
  - Implémentation,
  - Exploitation et maintenance,
  - Disposition.



- **des rôles et des responsabilités génériques** au nombre de huit: Utilisateurs, Maîtrise d'ouvrage, Maîtrise d'œuvre, Autorité d'homologation, Responsable de la sécurité des SI, Experts techniques, Comité de pilotage,

Commission d'homologation.

Les besoins de sécurité seront exprimés dans un dossier de sécurité qui servira de référence à l'autorité chargée de l'homologation. Ce dossier, régulièrement mis à jour pour refléter les évolutions du SI, contiendra l'ensemble des livrables produits au titre de l'application de la démarche proposée par le guide **GISSIP** tels que la fiche d'expression des objectifs de sécurité, la définition de la cible de sécurité, la politique de sécurité du SI, la documentation relative aux tests, aux évaluations de sécurité ou encore les tableaux de bord de sécurité du SI.

L'utilisation des outils méthodologiques développés par la **DCSSI** est fortement préconisée. Le tableau ci-contre liste les méthodologies, outils ou normes susceptibles d'être employés à chaque étape du cycle de vie.

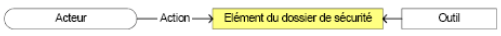
	1	2	3	4	5	6
EBIOS		X	X	X	X	X
FEROS			X	X		X
PSSI		X		X	X	X
TBDSSI				X	X	
ISO15408					X	

1: Opportunité
2: Faisabilité
3: Conception générale
4: Conception détaillée
5: Réalisation
6: Exploitation

Pour chacune de ces étapes, et pour chacun des niveaux de maturité, une fiche de synthèse est fournie qui précise les objectifs désignés, les pré-requis, les outils utilisables et les livrables à produire.

Le processus de traitement associé est décrit sous la forme d'un diagramme mettant en évidence les relations liant les acteurs, les livrables et les outils de production.

Un tableau récapitulatif est par ailleurs proposé (§ 4.9 - page 40) qui permet de visualiser d'un seul coup d'œil l'ensemble des actions et des livrables pour chaque niveau de maturité. L'utilisation d'un pictogramme permet de différencier les actions (pictogramme: carré) des livrables (pictogramme: flèche).

Étape	*Étape du cycle de vie générique des SI et niveau de maturité SSI visé*
Objectif	*Objectif général de l'étape en terme de SSI*
Préalables	*Actions ou documents nécessaires en entrée de l'étape*
Description	*Description des actions SSI à mener lors de l'étape*
Livrables	*Documents livrables en sortie de l'étape*
Outils	*Outils (méthodes, catalogues…) pouvant aider à la réalisation de l'étape*
Synthèse	*Schéma présentant les principaux acteurs, outils et livrables (composant le dossier de sécurité)* 

Une première annexe présente les analogies qui peuvent être établies entre les livrables de la démarche **GISSIP** et d'autres démarches d'homologation:

- Pour la **France** avec l'instruction **IGI 900** '*La sécurité des systèmes d'information qui font l'objet d'une classification de défense pour eux-mêmes ou pour les informations traitées*', l'instruction **II 920** '*Instruction interministérielle relative aux systèmes traitant des informations classifiées de défense de niveau confidentiel défense*' ou encore l'instruction **IGI 1300** '*Instruction générale interministérielle sur la protection du secret de la défense nationale*'.
- Dans le cadre de l'**OTAN** avec la directive **1014** '*Lignes directrices concernant la structure et le contenu de la procédure d'exploitation de sécurité des systèmes d'information et de communication*', la directive **1015** '*Lignes directrices pour l'établissement des énoncés des impératifs de sécurité*' ou encore la directive **1021** '*Lignes directrices pour l'approbation ou l'homologation de sécurité des systèmes d'information et de communication*'.

GISSIP (approche générique)	Homologation France	Homologation OTAN
Note d'orientation SSI	❑ Note d'orientation SSI	❑ Processus structuré validé par l'homologation de sécurité du SI ❑ Saisine de l'Autorité nationale de sécurité (ANS)
Note de stratégie de sécurité	❑ Note de stratégie de sécurité	❑ Note de stratégie de sécurité
FEROS	❑ FEROS	❑ *System-specific Security Requirement Statement* (SSRS)
Liste de meilleures pratiques	❑ Aucun	❑ Aucun
PSSI	❑ PSSI ❑ Protocole d'accord ❑ PSSI communautaire ❑ PSSI d'interconnexion	❑ SSRS ❑ *Community Security Requirement Statement* (CSRS) ❑ Accords de sécurité ❑ *System Interconnection Security Requirement Statement* (SISRS)
Cible de sécurité	❑ Cible de sécurité système ❑ Plan de sécurité système selon l'avancement du projet	❑ SSRS
Documents d'application de la PSSI	❑ PSSI du système ❑ Procédures d'exploitation de sécurité (PES)	❑ *Security OPerating ProcedureS* (SecOPs)
Documentation relative aux tests	❑ Plan Test générique	❑ Plan Test approuvé ❑ Rapport d'inspection de sécurité
Documentation relative aux évaluations	❑ Cible de sécurité produit	❑ *System-specific Electronic Information Security Requirement Statement* (SEISRS)
Décision d'homologation	❑ Décision d'homologation	❑ Proposition de *Statement of Compliance* (SoC) d'homologation
TDBSSI	❑ Aucun	❑ Aucun

On trouvera, en annexe du document, un glossaire Français/Anglais des termes employées (12 entrées), une liste d'acronymes (18 entrées) ainsi qu'un formulaire à utiliser pour transmettre à la DCSSI d'éventuels commentaires ou remarques sur le document.

- **Complément d'information**

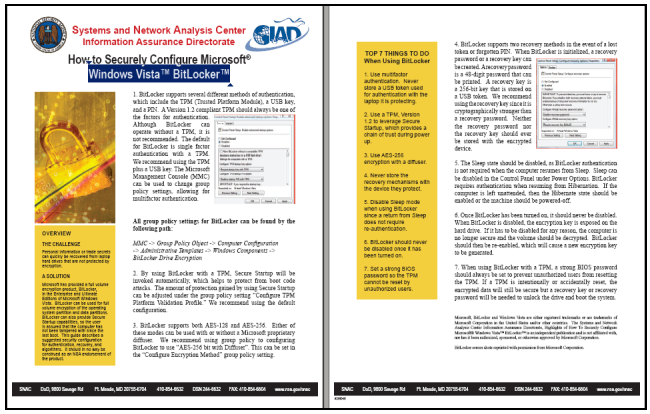
http://www.ssi.gouv.fr/fr/index.html
http://www.ssi.gouv.fr/fr/confiance/documents/methodes/GISSIP-Methode-2006-12-11.pdf
http://csrc.nist.gov/publications/nistpubs/800-64/NIST-SP800-64.pdf
http://www.ssi.gouv.fr/fr/confiance/dsis.html

METHODE

NSA - HOW TO SECURELY CONFIGURE MICROSOFT WINDOWS VISTA BITLOCKER

- **Description**

La **NSA** a publié un nouveau mémento de 2 pages intitulé '**How to Securely Configure Microsoft Windows Vista BitLocker**'. Celui-ci décrit les opérations à effectuer pour activer le mécanisme de chiffrement des données dénommé 'BitLocker' intégré au système d'exploitation **Vista** dans ses versions **Entreprise** (Enterprise) et **Intégrale** (Ultimate).



Outre l'activation du mécanisme de chiffrement, ce mémento recommande l'utilisation de l'algorithme **AES-256** en sélectionnant l'algorithme de diffusion dit '**Elephant**'.

Le choix d'une clef de recouvrement (256 bits) en lieu et place d'un simple mot de passe est conseillé pour limiter le risque d'une recherche exhaustive ou d'une divulgation. Ceci requiert l'utilisation d'un dispositif de sauvegarde amovible, une clef **USB** en l'occurrence, et donc la mise en place d'une procédure de stockage sécurisé de celui-ci.

Parmi les autres recommandations, on notera celles concernant la version du module **TPM** – l'utilisation de la version 1.2 est conseillée – ou encore la désactivation de la mise en veille simple, l'authentification **BitLocker** n'étant pas requise lors du réveil.

Ce n'est, semble-t-il, pas le cas si l'on active le mode hibernation. Il faudra aussi veiller à ne pas désactiver le mécanisme **BitLocker** et à protéger l'accès au **BIOS** par un mot de passe robuste pour éviter une réinitialisation de la configuration du TPM par une personne non autorisée. Les données ne seraient pas pour autant perdues mais il faudra faire appel à la clef de recouvrement pour pouvoir y accéder de nouveau.

- **Complément d'information**

http://www.nsa.gov/snac/support/I731-020R-2007.pdf - How to Securely Configure Microsoft Windows Vista BitLocker

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 à l'environnement '**HP-UX**'.

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	V1.2	Outil existant
Windows 2003 Member Servers	P1	V1.2	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
M	**HP-UX** 10.20, 11.00 et 11.11	**P1**	**V1.4**	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	P1	V2.1.3	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	P1 P2	V2.2	Outil existant
CISCO CAR	*P1 P2*		
CheckPoint FW1/VPN1	*P1 P2*		

Recommandations Applications			
Apache WEB serveur version 1.3 et 2.0	P1 P2	V1.7	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 P2	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	*P2*		

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_v2.0.8	tar	V2.08	LINUX

- **Complément d'information**

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

NIST – ETAT DES GUIDES DE LA SERIE SP800

- **Description**

Le **NIST** publie la version finale du document **SP800-95** '**Guide to Secure Web Services**' et une nouvelle version du **SP800-28** '**Guidelines on Active Content and Mobile Code**' pour commentaires.

SP800-12	An Introduction to Computer Security: The NIST Handbook	[R]	10/1995
SP800-18.1	Guide for Developing Security Plans for Federal Information Systems	[R]	08/2005
SP800-21.1	Guideline for Implementing Cryptography in the Federal Government	[D]	09/2005
SP800-26	Security Self-Assessment Guide for Information Technology Systems	[F]	11/2001
SP800-26.1	Guide for Inform. Security Program Assessments & System Reporting Form	[R]	08/2005
SP800-27a	Engineering Principles for Information Technology Security – Rev A	[F]	06/2004
SP800-28V2	**Guidelines on Active Content and Mobile Code**	[R]	09/2007
SP800-29	Comparison of Security Reqs for Cryptographic Modules in FIPS 140-1 & 140-2	[F]	10/2001
SP800-30	Underlying Technical Models for Information Technology Security – Rev A	[F]	01/2004
SP800-31	Intrusion Detection Systems	[F]	11/2001
SP800-32	Introduction to Public Key Technology and the Federal PKI Infrastructure	[F]	02/2001
SP800-33	Underlying Technical Models for Information Technology Security	[F]	12/2001
SP800-34	Contingency Planning Guide for Information Technology Systems	[F]	06/2002
SP800-35	Guide to Selecting IT Security Products	[F]	10/2003
SP800-36	Guide to IT Security Services	[F]	10/2003
SP800-37	Guidelines for the Security C&A of Federal Information Technology Systems	[F]	04/2004
SP800-38A	Recommendation for Block Cipher Modes of Operation – Method and Techniques	[F]	12/2001
SP800-38B	Recommendation for Block Cipher Modes of Operation – RMAC	[D]	12/2001
SP800-38C	Recommendation for Block Cipher Modes of Operation – CCM	[F]	05/2004
SP800-38D	Recommendation for Block Cipher Modes of Operation – GCM	[R]	04/2006

SP800-40	Applying Security Patches	[F]	09/2002
SP800-40-2	Creating a Patch and Vulnerability Management Program	[F]	11/2005
SP800-41	Guidelines on Firewalls and Firewall Policy	[F]	01/2002
SP800-42	Guidelines on Network Security testing	[F]	10/2003
SP800-43	System Administration Guidance for Windows2000	[F]	11/2002
SP800-44V2	Guidelines on Securing Public Web Servers	[R]	06/2007
SP800-45V2	Guide On Electronic Mail Security	[F]	02/2007
SP800-46V2	Security for Telecommuting and Broadband Communications	[R]	06/2007
SP800-47	Security Guide for Interconnecting Information Technology Systems	[F]	09/2002
SP800-48r1	Wireless Network Security: 802.11, Bluetooth™ and Handheld Devices	[R]	08/2007
SP800-49	Federal S/MIME V3 Client Profile	[F]	11/2002
SP800-50	Building an Information Technology Security Awareness & Training Program	[F]	03/2003
SP800-51	Use of the Common Vulnerabilities and Exposures Vulnerability Naming Scheme	[F]	09/2002
SP800-52	Guidelines on the Selection and Use of Transport Layer Security	[D]	09/2004
SP800-53-1	Recommended Security Controls for Federal Information Systems	[M]	12/2006
SP800-53A	Guide for Assessing the Security Controls in Federal Information Systems	[R]	06/2007
SP800-54	Border Gateway Protocol Security	[F]	07/2007
SP800-55	Security Metrics Guide for Information Technology Systems	[F]	07/2003
SP800-56A	Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography	[M]	05/2006
SP800-57	Recommendation for Key Management, Part 1: General Guideline	[F]	08/2005
	Recommendation for Key Management, Part 2: Best Practices	[F]	08/2005
SP800-58	Security Considerations for Voice Over IP Systems	[F]	03/2005
SP800-59	Guideline for Identifying an Information System as a National Security System	[F]	08/2003
SP800-60	Guide for Mapping Types of Information & Information Systems to Security Categories	[F]	06/2004
SP800-61	Computer Security Incident Handling Guide	[F]	01/2004
SP800-63	Recommendation for Electronic Authentication	[M]	04/2006
SP800-64	Security Considerations in the Information System Development Life Cycle	[F]	07/2004
SP800-65	Recommended Common Criteria Assurance Levels	[F]	01/2005
SP800-66	An Introductory Resource Guide for Implementing the HIPAA Security Rule	[F]	03/2005
SP800-67	Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher	[F]	05/2004
SP800-68	Guidance for Securing Microsoft Windows XP Systems for IT Professionals	[F]	10/2005
SP800-69	Guidance for Securing Microsoft Windows XP Home Edition	[R]	08/2006
SP800-70	The NIST Security Configuration Checklists Program	[F]	05/2005
SP800-72	Guidelines on PDA Forensics	[F]	11/2004
SP800-73	Integrated Circuit Card for Personal Identity Verification	[R]	01/2005
SP800-73-1	Interfaces to Personal Identity Verification	[M]	04/2007
SP800-76-1	Biometric Data Specification for Personal Identity Verification	[F]	01/2007
SP800-77	Guide to Ipsec VPNs	[F]	12/2005
SP800-78-1	Cryptographic Algorithms and Key Sizes for Personal Identity Verification	[R]	07/2006
SP800-79	Guidelines for Certification & Accreditation of PIV Card Issuing Organizations	[F]	07/2005
SP800-80	Guide for Developing Performance Metrics for Information Security	[R]	05/2006
SP800-81	Secure Domain Name System (DNS) Deployment Guide	[D]	05/2006
SP800-82	Guide to SCADA and Industrial Control Systems Security	[R]	09/2006
SP800-83	Guide to Malware Incident Prevention and Handling	[F]	11/2005
SP800-84	Guide to Single-Organization IT Exercises	[R]	08/2005
SP800-85B	PIV Middleware and PIV Card Application Conformance Test Guidelines	[F]	07/2006
SP800-86	Computer, Network Data Analysis: Forensic Techniques to Incident Response	[F]	08/2006
SP800-87	Codes for the Identification of Federal and Federally-Assisted Organizations	[F]	03/2007
SP800-88	Guidelines for Media Sanitization	[M]	08/2006
SP800-89	Recommendation for Obtaining Assurances for Digital Signature Applications	[F]	11/2006
SP800-90	Random Number Generation Using Deterministic Random Bit Generators	[F]	06/2006
SP800-92	Guide to Computer Security Log Management	[R]	04/2006
SP800-94	Guide to Intrusion Detection and Prevention (IDP) Systems	[F]	02/2007
SP800-95	**Guide to Secure Web Services**	[F]	08/2007
SP800-96	PIV Card / Reader Interoperability Guidelines	[M]	07/2006
SP800-97	Guide to IEEE 802.11i: Robust Security Networks	[F]	02/2007
SP800-98	Guidance for Securing Radio Frequency Identification (RFID) Systems	[F]	04/2007
SP800-100	Information Security Handbook: A Guide for Managers	[M]	03/2007
SP800-101	Guidelines on Cell Phone Forensics	[F]	05/2007
SP800-103	An Ontology of Identity Credentials, Part I: Background and Formulation	[R]	09/2006
SP800-104	A Scheme for PIV Visual Card Topography	[F]	06/2007

SP800-106	Randomized Hashing Digital Signatures	[R]	07/2007
SP800-107	Recommendation for Using Approved Hash Algorithms	[R]	07/2007
SP800-111	Guide to Storage Encryption Technologies for End User Devices	[R]	08/2007
SP800-113	Guide to SSL VPNs	[R]	08/2007

[F] Finalisé **[*]** Récemment finalisé **[M]** Mise à jour
[R] Pour commentaire et relecture **[D]** En cours de développement

- **Complément d'information**

http://csrc.nist.gov/publications/nistpubs/index.html - Catalogue
http://csrc.nist.gov/publications/nistpubs/800-95/SP800-95.pdf - SP800-95 version finale
http://csrc.nist.gov/publications/drafts/sp800-28-rev2/Draft-SP800-28v2.pdf - SP800-28V2 proposition

NSA - CATALOGUE DES GUIDES DE SECURITE

- **Description**

La parution du mémento intitulé '**How to Securely Configure Microsoft Windows Vista BitLocker**' nous conduit à proposer une mise à jour de notre catalogue des publications de la **NSA**.

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					
N	R	**Windows Vista Security Guide**	-	25/10/2006	MIC
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
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
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
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
Base 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	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
	I	So Your Boss Bought you a New Laptop How do you identify & disable wireless capabilities		04/06/2007	NSA
N	I	**How to Securely Configure Microsoft Windows Vista BitLocker**		15/09/2007	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

- **Complément d'information**

http://www.nsa.gov/snac/ - Portail d'accès aux guides
http://www.nsa.gov/snac/support/I731-020R-2007.pdf - Notice BitLocker

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.

RÉSEAU

Nom	Fonction	Ver.	Date	Source
BIND	Gestion de Nom (DNS)	9.4.1	30/04/07	http://www.isc.org/
DHCP	Serveur d'adresse	3.1.0	19/07/07	http://www.isc.org/
NTP4	Serveur de temps	4.2.4	07/03/07	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	2006k	29/08/07	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	8.14.1	04/04/07	ftp://ftp.sendmail.org/pub/sendmail/

WEB

Nom	Fonction	Ver.	Date	Source
APACHE	Serveur WEB	1.3.39	04/09/07	http://httpd.apache.org/dist
		2.0.61	04/09/07	
		2.2.6	04/09/07	
ModSSL	API SSL Apache 1.3.39	2.8.30	12/09/07	http://www.modssl.org
MySQL	Base SQL	5.1.22	14/09/07	http://dev.mysql.com/doc/refman/5.1/en/news.html
SQUID	Cache WEB	2.6s16	05/09/07	http://www.squid-cache.org/Versions/

AUTRE

Nom	Fonction	Ver.	Date	Source
FreeRadius	Gestion de l'identité	1.1.7	25/07/07	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	2.3.38	20/08/07	ftp://ftp.openldap.org/pub/OpenLDAP/openldap-release/
Samba	Gestion de fichiers	3.0.26	11/09/07	http://us1.samba.org/samba/
Tor	Anonymat	0.1.2.17	02/09/07	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	1.8.6	13/03/07	http://www.ruby-lang.org/en/downloads/
PHP	WEB Dynamique	5.2.4	30/08/07	http://www.php.net/downloads.php

ANALYSE RÉSEAU

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	0.99.6	09/07/07	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	4.0.1	30/07/07	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
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 Sécurité

Nom	Fonction	Ver.	Date	Source
BackTrack	Boîte à outils	2.0	06/03/07	http://www.remote-exploit.org/backtrack_download.html
curl	Analyse http et https	7.17.0	13/09/07	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	1.36	15/02/07	http://www.cirt.net/nikto/
nmap	Vulnérabilité réseau	4.22soc6	29/08/07	http://www.insecure.org/nmap/nmap_changelog.html
Saint	Vulnérabilité réseau	6.6	12/09/07	http://www.saintcorporation.com/resources/updates.html
Sara	Vulnérabilité réseau	7.4.2	01/09/07	http://www-arc.com/sara/
Wikto	Analyse http et https	2.0.2778	10/08/07	http://www.sensepost.com/research/wikto/
Whisker	LibWhisker	2.4	03/07	http://www.wiretrip.net/rfp/lw.asp

Confidentialité

Nom	Fonction	Ver.	Date	Source
GPG	Signature/Chiffrement	2.0.7	10/09/07	http://www.gnupg.org/(fr)/news.html
GPG4Win	Signature/Chiffrement	1.0.6	29/08/06	http://www.gnupg.org/(fr)/news.html
GPG S/MIME	Signature/Chiffrement	1.9.20	20/12/05	http://www.gnupg.org/(fr)/news.html
LibGCrypt	Signature/Chiffrement	1.2.3	29/08/06	http://www.gnupg.org/(fr)/news.html

Contrôle d'Accès Réseau

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

Contrôle d'Intégrité

Nom	Fonction	Ver.	Date	Source
RootKit hunt	Compromission UNIX	1.2.9	17/06/07	http://www.rootkit.nl/projects/rootkit_hunter.html
ChkRootKit	Compromission UNIX	0.47	10/10/06	http://www.chkrootkit.org/
RKRevealer	Compromission WIN	1.71	01/11/06	http://www.microsoft.com/technet/sysinternals/default.mspx

Détection 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	2.7.0.1	06/08/07	http://www.snort.org/dl/

Générateurs 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	1.1.1	09/04/07	http://www.secdev.org/projects/scapy/files/

Pare-Feux

Nom	Fonction	Ver.	Date	Source
DrawBridge	PareFeu FreeBsd	4.0	23/04/04	http://drawbridge.tamu.edu
IpFilter	Filtre datagramme	4.1.26	09/07	http://coombs.anu.edu.au/ipfilter/ip-filter.html
NetFilter	Pare-Feu IpTables	1.3.8	25/06/07	http://www.netfilter.org/projects/iptables/downloads.html

Tunnels

Nom	Fonction	Ver.	Date	Source
CIPE	Pile Crypto IP (CIPE)	1.6	04/08/04	http://sites.inka.de/sites/bigred/devel/cipe.html
http-tunnel	Encapsulation http	3.0.5	06/12/00	http://www.nocrew.org/software/httptunnel.html
OpenSSL	Pile SSL	0.9.8e	23/02/07	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	4.20	30/11/06	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 **30/08/2007** au **27/09/2007**, **34 RFC** ont été publiés dont 7 RFC ayant trait à la sécurité.

RFC TRAITANT DE LA SÉCURITÉ

Thème	Num	Date	Etat	Titre
DNS	5011	09/07	Pst	Automated Updates of DNS Security (DNSSEC) Trust Anchors
IMAP	4959	09/07	Pst	IMAP Extension for Simple Authentication and Security Layer (SASL) Initial Client Response
IPV6	4941	09/07	Dft	Privacy Extensions for Stateless Address Autoconfiguration in IPv6
	4942	09/07	Inf	IPv6 Transition/Co-existence Security Considerations
	4943	09/07	Inf	IPv6 Neighbor Discovery On-Link Assumption Considered Harmful
OCSP	5019	09/07	Pst	The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments
SMIME	5008	09/07	Inf	Suite B in Secure/Multipurpose Internet Mail Extensions (S/MIME)

RFC TRAITANT DE DOMAINES CONNEXES A LA SECURITE

Thème	Num	Date	Etat	Titre
IMAP	5032	09/07	Pst	WITHIN Search Extension to the IMAP Protocol
SCTP	5061	09/07	Pst	Stream Control Transmission Protocol (SCTP) Dynamic Address Reconfiguration

AUTRES RFC

Thème	Num	Date	Etat	Titre
AII	5003	09/07	Pst	Attachment Individual Identifier (AII) Types for Aggregation
BFCP	5018	09/07	Pst	Connection Establishment in the Binary Floor Control Protocol (BFCP)
BGP	5004	09/07	Pst	Avoid BGP Best Path Transitions from One External to Another
DHCP	4994	09/07	Pst	DHCPv6 Relay Agent Echo Request Option
	5007	09/07	Pst	DHCPv6 Leasequery
	5010	09/07	Pst	The Dynamic Host Configuration Protocol Version 4 (DHCPv4) Relay Agent Flags Suboption
IETF	4965	09/07	Inf	CableLabs - IETF Standardization Collaboration
	5005	09/07	Pst	Feed Paging and Archiving
IPV6	4861	09/07	Dft	Neighbor Discovery for IP version 6 (IPv6)
	4862	09/07	Dft	IPv6 Stateless Address Autoconfiguration
	4944	09/07	Pst	Transmission of IPv6 Packets over IEEE 802.15.4 Networks
	5006	09/07	Exp	IPv6 Router Advertisement Option for DNS Configuration
	5014	09/07	Inf	IPv6 Socket API for Source Address Selection
	5072	09/07	Dft	IP Version 6 over PPP
ISIS	5029	09/07	Pst	Definition of an IS-IS Link Attribute Sub-TLV
MIB	5017	09/07	Pst	MIB Textual Conventions for Uniform Resource Identifiers (URIs)
MPLS	4990	09/07	Inf	Use of Addresses in Generalized Multiprotocol Label Switching (GMPLS) Networks
MSCML	5022	09/07	Inf	Media Server Control Markup Language (MSCML) and Protocol
MSRP	4975	09/07	Pst	The Message Session Relay Protocol (MSRP)
	4976	09/07	Pst	Relay Extensions for the Message Sessions Relay Protocol (MSRP)
P2P	4981	09/07	Inf	Survey of Research towards Robust Peer-to-Peer Networks: Search Methods
SCTP	4960	09/07	Pst	Stream Control Transmission Protocol
SIP	4964	09/07	Inf	The P-Answer-State Header Extension to SIP for the Open Mobile Alliance Push to Talk over Cellular
	5009	09/07	Inf	Private Header (P-Header) Extension to SIP for Authorization of Early Media

LES DRAFTS

Du **30/08/2007**au **27/09/2007**, 169 drafts ont été publiés : **133** drafts mis à jour, **36** nouveaux drafts, dont **6** drafts ayant directement trait à la sécurité.

NOUVEAUX DRAFTS TRAITANT DE LA SECURITE

Thème	Nom du Draft	Date	Titre
CGA	draft-haddad-cgaext-optisend-00	19/09	Secure Neighbor Discovery Optimizations: The OptiSeND Protocol
BUNDLE	draft-irtf-dtnrg-bundle-checksum-00	18/09	Checksum Ciphersuites for the Bundle Protocol
EAP	draft-dondeti-dime-erp-diameter-00	23/09	Diameter Support for EAP Re-authentication Protocol
	draft-hanna-eap-ttls-agility-00	26/09	Key Agility Extensions for EAP-TTLSv0
KERB	draft-rabinovich-krb-wg-x509-name-...-00	24/09	Constraining Kerberos Names in X.509 Certificates
KEY	draft-ietf-keyprov-portable-symmetric-....-00	31/08	Portable Symmetric Key Container
MPLS	draft-ietf-mpls-mpls-and-gmpls-securit....-00	12/09	Security Framework for MPLS and GMPLS Networks

MISE A JOUR DE DRAFTS TRAITANT DE LA SECURITE

Thème	Nom du Draft	Date	Titre
CRYPTO	draft-williams-on-channel-binding-04	31/08	On the Use of Channel Bindings to Secure Channels
	draft-lepinski-dh-groups-01	14/09	Additional Diffie-Hellman Groups for use with IETF Standards
DNS	draft-weiler-dnssec-dlv-04	14/09	DNSSEC Lookaside Validation (DLV)
DTNRG	draft-irtf-dtnrg-bundle-security-04	21/09	Bundle Security Protocol Specification
EDIINT	draft-meadors-certificate-exchange-07	21/09	Certificate Exchange Messaging for EDIINT
IBCS	draft-martin-ibcs-07	26/09	Supersingular Curve Implement. of the BF & BB1 Cryptosystems
IPSEC	draft-ietf-btns-connection-latching-03	17/09	IPsec Channels: Connection Latching
IPV6	draft-ietf-mipshop-handover-key-02	26/09	Distributing a Symmetric FMIPv6 Handover Key using SEND
	draft-devarapalli-mip6-authprotocol-boo…-03	21/09	Mobile IPv6 Bootstrapping for the Authentication Option Protocol
KERB	draft-ietf-krb-wg-kerberos-set-passwd-07	25/09	Kerberos Set/Change Key/Password Protocol Version 2
KEY	draft-ietf-hokey-reauth-ps-03	10/09	Handover Key mgmt and Re-authentication Problem Statement
	draft-wing-media-security-requirements-05	20/09	Requirements and Analysis of Media Security Key Mgmt Protocols
PKIX	draft-ietf-pkix-scvp-33	21/09	Server-based Certificate Validation Protocol (SCVP)
RADIUS	draft-ietf-radext-fixes-08	13/09	Common RADIUS Implementation Issues and Suggested Fixes
RSERPOO	draft-ietf-rserpool-threats-08	19/09	Threats Introduced by Rserpool and Requirements for Security
SENDER	draft-kucherawy-sender-auth-header-07	21/09	Message Header Field for Indicating Message Auth. Status
SMIME	draft-ietf-smime-ibearch-05	26/09	Identity-based Encryption Architecture
	draft-ietf-smime-bfibecms-06	26/09	Using the Boneh-Franklin and Boneh-Boyen identity-based
	draft-ietf-smime-cms-auth-enveloped-06	21/09	CMS Authenticated-Enveloped-Data Content Type
	draft-ietf-smime-cms-aes-ccm-and-gcm-03	21/09	Using AES-CCM and AES-GCM Authenticated Encryption
SNMP	draft-ietf-isms-transport-security-model-06	21/09	Transport Security Model for SNMP
SPEER	draft-niccolini-speermint-voipthreats-02	31/08	VoIP Security Threats relevant to SPEERMINT
TA	draft-wallace-ta-mgmt-problem-statement-02	12/09	Trust Anchor Management Problem Statement
TLS	draft-housley-tls-authz-extns-07	10/09	Transport Layer Security (TLS) Authorization Extensions
	draft-ietf-tls-rfc4346-bis-05	18/09	The Transport Layer Security (TLS) Protocol Version 1.2

DRAFTS TRAITANT DE DOMAINES CONNEXES A LA SECURITE

Thème	Nom du Draft	Date	Titre
DIAMETER	draft-ietf-dime-diameter-api-04	26/09	The Diameter API
	draft-ietf-dime-rfc3588bis-07	10/09	Diameter Base Protocol
	draft-bodin-dime-auditing-reqs-03	10/09	Auditing Functionality in Diameter
ICE	draft-ietf-mmusic-ice-18	13/09	ICE: A Protocol for NAT Traversal for Offer/Answer Protocols
IDR	draft-ietf-idr-encaps-safi-00	31/08	BGP Encapsulation SAFI and BGP Tunnel Encapsulation Attribute
IP	draft-templin-inetmtu-01	25/09	Packetization Layer Path MTU Discovery for IP/*/IPv4 Tunnels
IPV6	draft-ietf-netlmm-proxymip6-06	24/09	Proxy Mobile IPv6
LDAP	draft-findlay-ldap-groupofentries-00	13/09	The LDAP groupOfEntries object class
MSTP	draft-melia-mipshop-mstp-solution-00	21/09	Mobility Services Transport Protocol Design
MTU	draft-templin-inetmtu-lite-00	26/09	Minimal Packetization Layer Path MTU Discovery for IP Tunnels
NAT	draft-ietf-behave-nat-icmp-05	26/09	NAT Behavioral Requirements for ICMP protocol
NETLMM	draft-jhlee-netlmm-heartbeatlma-00	31/08	Heartbeat Mechanism for Local Mobility Anchors in Proxy Mobile
PCE	draft-yasukawa-pce-vpn-req-03	31/08	PCC-PCE Communication Requirements for VPNs
RFC4214	draft-templin-rfc4214bis-05	10/09	Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)
RSVP	draft-ietf-tsvwg-rsvp-proxy-approaches-02	12/09	RSVP Proxy Approaches
XML	draft-frascone-xml-dictionary-00	26/09	Diameter XML Dictionary

AUTRES DRAFTS

Thème	Nom du Draft	Date	Titre
ATOM	draft-snell-atompub-feature-10	18/09	Atom Publishing Protocol Feature Discovery
AUTOCON	draft-mase-autoconf-framework-04	24/09	A common framework for autoconfiguration of ad hoc networks
BEHAVE	draft-denis-behave-rfc3489bis-test-vectors-02	21/09	Test vectors for RFC3489bis
CIDR	draft-terrell-cidr-net-descrpt-expands-…-21	10/09	The CIDR Network Descriptor expands the size of the IPtX …
DHCP	draft-ietf-dhc-option-guidelines-00	12/09	Guidelines for Creating New DHCP Options
DKIM	draft-ietf-dkim-ssp-01	17/09	DKIM Sender Signing Practices
DNS	draft-ietf-dnsext-rfc2672bis-dname-05	26/09	Update to DNAME Redirection in the DNS
	draft-irtf-asrg-dnsbl-04	19/09	DNS Based Blacklists and Whitelists for E-Mail
DTNRG	draft-irtf-dtnrg-sdnv-00	18/09	Using Self-Delimiting Numeric Values in Protocols
EAP	draft-tschofenig-eap-ikev2-14	10/09	EAP-IKEv2 Method
EMERG	draft-ietf-ecrit-phonebcp-02	19/09	BCP for Communications Services in support of Emergency Calling
	draft-ietf-ecrit-framework-03	19/09	Framework for Emergency Calling using Internet Multimedia
ENUM	draft-livingood-enum-videomsg-01	14/09	IANA Registration for an Enumservice for Video Messaging
	draft-livingood-enum-voicemsg-01	13/09	IANA Registration for an Enumservice for Voice Messaging
GEOPRIV	draft-ietf-geopriv-l7-lcp-ps-05	12/09	GEOPRIV Layer 7 Location Configuration Protocol
	draft-ietf-geopriv-lbyr-requirements-00	11/09	Requirements for a Location-by-Reference Mechanism
	draft-thomson-geopriv-3825bis-01	24/09	DHCP Option for Geodetic Location Information
	draft-thomson-geopriv-lis-discovery-03	26/09	Discovering the Local Location Information Server (LIS)
HTML	draft-daviel-html-geo-tag-07	10/09	Geographic registration of HTML documents
HTTP	draft-snell-http-prefer-00	18/09	Prefer Header for HTTP
HUNTER	draft-thomas-hunter-reed-ospf-lite-00	31/08	OSPF-lite
IETF	draft-ietf-opsawg-operations-and-….-00	19/09	Considering Operations and Management of New Protocols
IP	draft-aboba-ip-config-02	18/09	Principles of Internet Host Configuration
	draft-manner-router-alert-iana-00	18/09	IANA Considerations for the IPv4 and IPv6 Router Alert Option

	draft-ietf-rtgwg-ipfrr-spec-base-09	21/09	Basic Specification for IP Fast-Reroute: Loop-free Alternates
IPFIX	draft-ietf-ipfix-implementation-guidelines-07	26/09	IPFIX Implementation Guidelines
IPPM	draft-ietf-ippm-storetraceroutes-05	26/09	Information Model and XML Data Model for Traceroute Meas…
IPTX	draft-terrell-iptx-mx-dhcp-specification-02	10/09	The IPtX Dynamic Host Configuration Protocol; DHCPvIPtX-MX
IPV4	draft-ietf-mip4-dsmipv4-04	24/09	Dual Stack Mobile IPv4
	draft-ietf-mip4-nemo-v4-base-02	12/09	Network Mobility (NEMO) Extensions for Mobile IPv4
	draft-ietf-mip4-generic-notification-…02	11/09	Generic Notification Message for Mobile IPv4
	draft-reitzel-ipv4-source-routing-is-evil-00	11/09	Deprecation of Source Routing Options in IPv4
	draft-makela-mip4-nemo-haaro-00	14/09	Home Agent assisted Route Optimization between Mobile IPv4 Net
IPV6	draft-ietf-ipv6-ra-flags-option-02	14/09	IPv6 Router Advertisement Flags Option
	draft-ietf-mip6-hiopt-07	21/09	DHCP Option for Home Information Discovery in MIPv6
	draft-ietf-mip6-experimental-messages-02	24/09	Mobile IPv6 Experimental Messages
	draft-ietf-mip6-vsm-02	24/09	Mobile IPv6 Vendor Specific Option
IURN	draft-goodwin-iso-urn-02	11/09	A Uniform Resource Name (URN) Namespace for the ISO
JABBERID	draft-saintandre-jabberid-06	14/09	The Jabber-ID Header Field
L2VPN	draft-ietf-l2vpn-oam-req-frmk-09	21/09	L2VPN OAM Requirements and Framework
	draft-ietf-l2vpn-vpls-mcast-reqts-05	12/09	Requirements for Multicast Support in Virtual Private LAN Services
	draft-ietf-l2vpn-vpls-mcast-02	21/09	Multicast in VPLS
LDAP	draft-legg-ldap-transfer-06	21/09	LDAP: Transfer Encoding Options
LDP	draft-brockners-ldp-half-duplex-mp2mp-01	21/09	LDP Extensions for Half-Duplex Multipoint-to-MPLS
LEMONAD	draft-ietf-lemonade-streaming-03	21/09	Streaming Internet Messaging Attachments
LISP	draft-meyer-lisp-cons-02	10/09	A Content distribution Overlay Network Service for LISP
MANET	draft-ietf-manet-packetbb-09	10/09	Generalized MANET Packet/Message Format
	draft-templin-autoconf-dhcp-09	25/09	MANET Autoconfiguration
MATH	draft-terrell-math-quant-ternary-logic….-12	21/09	The Mathematics of Quantification, and the Rudiments Of the …
MBONED	draft-ietf-mboned-routingarch-10	25/09	Overview of the Internet Multicast Routing Architecture
MIME	draft-conboy-mime-ocf-00	10/09	Media Type Registrations for OEBPS Containger Format (OCF)
MPLS	draft-ietf-ccamp-inter-domain-rsvp-te-07	24/09	Inter domain MPLS and GMPLS Traffic Engineering - RSVP-TE ext.
	draft-ietf-ccamp-mpls-gmpls-interwork…-04	24/09	Framework for MPLS-TE to GMPLS migration
	draft-ietf-ccamp-mpls-gmpls-interwork…-02	24/09	Interworking Requirements to Support operation of MPLS-TE
	draft-ietf-ccamp-inter-domain-recovery…-02	13/09	Analysis of Inter-domain Label Switched Path (LSP) Recovery
	draft-ietf-mpls-p2mp-te-mib-05	24/09	Point-to-Multipoint MPLS TE MIB module
	draft-ietf-mpls-rsvp-te-no-php-oob-….-00	18/09	Non PHP Behavior and out-of-band mapping for RSVP-TE LSPs
	draft-yasukawa-pce-p2mp-req-03	31/08	PCC-PCE Communication Requirements for Point to MPLS-TE
	draft-yasukawa-mpls-mp2p-rsvpte-03	31/08	Supporting Multipoint-to-Point Label Switched Paths in MPLS-TE
	draft-bernstein-ccamp-wavelength-…01	14/09	GMPLS and PCE Control of Wavelength Switched Optical Networks
MSEC	draft-ietf-msec-gdoi-update-03	18/09	Updates to the Group Domain of Interpretation (GDOI)
MSRP	draft-denis-simple-msrp-comedia-00	25/09	Connection setup negociation for the MSRP
NAT	draft-ietf-behave-rfc3489bis-10	13/09	Session Traversal Utilities for (NAT) (STUN)
	draft-ietf-behave-multicast-10	10/09	IP Multicast Requirements for NAT
	draft-ietf-behave-p2p-state-04	26/09	State of Peer-to-Peer(P2P) Communication Across NAT
ND	draft-wbeebee-on-link-and-off-link-…-00	10/09	ND On-link and Off-link Determination
	draft-wbeebee-nd-implementation-…-00	10/09	Known ND Implementation Problems
	draft-wbeebee-nd-updates-00	10/09	Data Forwarding and Address Resolution Updates to 2461bis
NERD	draft-lear-lisp-nerd-02	21/09	NERD: A Not-so-novel EID to RLOC Database
NETCONF	draft-ietf-netconf-notification-09	11/09	NETCONF Event Notifications
	draft-iijima-ngo-vlandatamodel-01	31/08	VLAN data model for NETCONF
NFS	draft-ietf-nfsv4-minorversion1-14	25/09	NFSv4 Minor Version 1
NID	draft-schuetz-nid-arch-00	18/09	Node Identity Internetworking Architecture
NTP	draft-ietf-ntp-autokey-00	25/09	Network Time Protocol Version 4 Autokey Specification
OSPF	draft-acee-ospf-multi-instance-00	10/09	OSPF Multi-Instance Extensions
	draft-ietf-ospf-ospfv3-mib-12	21/09	Management Information Base for OSPFv3
	draft-ietf-ospf-ospfv3-traffic-09	21/09	Traffic Engineering Extensions to OSPF version 3
PCE	draft-ietf-pce-inter-layer-frwk-05	21/09	Framework for PCE-Based Inter-Layer MPLS and GMPLS TE
	draft-ietf-pce-disco-proto-isis-08	24/09	IS-IS Protocol Extensions for PCE Discovery
	draft-ietf-pce-disco-proto-ospf-08	24/09	OSPF Protocol Extensions for PCE Discovery
	draft-ietf-pce-tc-mib-02	25/09	Definitions of Textual Conventions for Path Computation Element
	draft-ietf-pce-manageability-requirements-02	31/08	Inclusion of Manageability Sections in PCE Working Group Drafts
	draft-ietf-pce-path-key-01	12/09	Preserving Topology Confidentiality in Inter-Domain Path …
	draft-ietf-pce-of-00	10/09	Encoding of Objective Functions in PCE communication
	draft-ietf-pce-monitoring-00	21/09	A set of monitoring tools for PCE based Architecture
PPPOE	draft-bberry-pppoe-scaled-credits-metrics-00	14/09	PPPoE Extensions for Scaled Credits and Link Metrics
PWE3	draft-ietf-pwe3-pw-mib-12	24/09	Pseudowire (PW) Management Information Base
	draft-ietf-pwe3-pw-tc-mib-12	24/09	Textual Conventions and for Managing Pseudowires over PSN
	draft-ietf-pwe3-vccv-15	21/09	Pseudowire VCCV A Control Channel for Pseudowires
	draft-ietf-pwe3-tdm-control-protocol-…04	12/09	Control Protocol Extensions for Setup of TDM Pseudowires
	draft-ietf-pwe3-fc-encap-05	18/09	Encapsulation Methods for Transport of Fibre Channel frames
	draft-ietf-pwe3-mpls-transport-01	10/09	Application of Ethernet Pseudowires to MPLS Transport Networks
RFC2026	draft-carpenter-rfc2026-changes-01	24/09	Proposed Changes to RFC 2026
ROHC	draft-ietf-rohc-sigcomp-sip-08	20/09	Applying SigComp to the Session Initiation Protocol (SIP)
RSERPOO	draft-ietf-rserpool-asap-17	22/09	Aggregate Server Access Protocol (ASAP)
	draft-ietf-rserpool-enrp-17	22/09	Endpoint Handlespace Redundancy Protocol (ENRP)
	draft-ietf-rserpool-common-param-13	22/09	ASAP and ENRP Parameters
	draft-ietf-rserpool-policies-06	22/09	Reliable Server Pooling Policies
RTP	draft-ietf-avt-rtp-jpeg2000-18	12/09	RTP Payload Format for JPEG 2000 Video Streams
	draft-ietf-avt-rtp-jpeg2000-beam-09	12/09	Extensions for Scalability and Main Header Recovery
	draft-ietf-avt-rtp-uemclip-01	21/09	RTP payload format for UEMCLIP speech codec

	draft-ietf-avt-forward-shifted-red-00	21/09	Forward-shifted RTP Redundancy Payload Support
SAVA	draft-wu-sava-testbed-experience-02	24/09	SAVA Testbed and Experiences to Date
SIEVE	draft-melnikov-sieve-notify-sip-message-00	31/08	Sieve Notification Mechanism: SIP MESSAGE
SIP	draft-salsano-sipping-siphandover-solution-01	31/08	A solution for vertical handover of multimedia sessions using SIP
	draft-vanelburg-sipping-served-user-02	21/09	The SIP P-Served-User Private-Header (P-Header)
	draft-ietf-sipping-race-examples-04	31/08	Examples call flow in race condition on Session Initiation Protocol
SMIME	draft-ietf-smime-cades-05	18/09	CMS Advanced Electronic Signatures (CAdES)
SMING	draft-schoenw-sming-lessons-01	25/09	Protocol Independent Network Mgmt Data Modeling Languages
SMS	draft-wilde-sms-uri-13	24/09	URI Scheme for GSM Short Message Service
SNMP	draft-ietf-isms-tmsm-10	18/09	Transport Subsystem for SNMP
TCP	draft-larsen-tsvwg-port-randomization-02	10/09	Port Randomization
TGREP	draft-ietf-iptel-tgrep-09	21/09	A Telephony Gateway REgistration Protocol (TGREP)
TICTOC	draft-bryant-tictoc-probstat-01	24/09	TICTOC Problem Statement
UDP	draft-ietf-tsvwg-udp-guidelines-03	19/09	UDP Usage Guidelines for Application Designers
	draft-ietf-tsvwg-udplite-mib-01	11/09	MIB for the UDP-Lite protocol
UNICODE	draft-crispin-collation-unicasemap-07	31/08	i;unicode-casemap - Simple Unicode Collation Algorithm
XBE32	draft-uruena-xbe32-02	10/09	eXtensible Binary Encoding (XBE32)
XED	draft-legg-xed-roadmap-06	31/08	The XML-Enabled Directory
	draft-legg-xed-schema-05	31/08	The XML-Enabled Directory
	draft-legg-xed-protocols-05	31/08	The XML-Enabled Directory: Protocols

NOS COMMENTAIRES

LES RFC

RFC4949

Internet Security Glossary, Version 2

En mai 2000 paraissait le **RFC2828** intitulé **Internet Security Glossary**. (Rapport N°19 – Février 2000). Edité par **R.W Shirey**, qui travaillait alors pour la société '**BBN Technologies**' le fournisseur des premiers équipements constituant l'ancêtre de l'Internet, ce remarquable glossaire contenait la définition de 1050 termes couramment utilisés dans le domaine de la sécurité de l'Internet.

En 2004, **R.W Shirey** s'engageait dans un long et fastidieux travail de mise à jour conduisant à la publication le mois dernier de la seconde édition de ce glossaire. La version 2 s'est ainsi enrichie de quelques 607 nouvelles entrées (1657 termes au total) telles que: *salami swindle*, *sandbox*, *weak key* ou encore *zombie*.

La structure du document reste inchangée. Chaque entrée est précédée du caractère délimiteur '$' facilitant l'extraction automatique des définitions. Plusieurs définitions peuvent être proposées pour un même terme qui reflètent sa signification à travers différents contextes d'utilisation.

Quatre classes sont ainsi définies et préfixées par un caractère spécifique:

Classe '**I**' : Terme utilisé en référence à l'Internet,
Classe '**N**' : Terme utilisé en dehors du cadre spécifique de l'Internet
Classe '**O**' : Autres définitions
Classe '**D**' : Termes dépréciés ou obsolètes

Nous proposons ci-dessous, la définition du terme '**threat**' dans la première et seconde édition du glossaire ce qui permettra au lecteur de se faire une idée de la qualité du travail et de l'effort investi dans l'établissement de ce document de référence.

Définitions du RFC2828

$ **threat**

(**I**) A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. (See: attack, threat action, threat consequence.)

(**C**) That is, a threat is a possible danger that might exploit a vulnerability. A threat can be either "intentional" (i.e., intelligent; e.g., an individual cracker or a criminal organization) or "accidental" (e.g., the possibility of a computer malfunctioning, or the possibility of an "act of God" such as an earthquake, a fire, or a tornado).

(**C**) In some contexts, such as the following, the term is used narrowly to refer only to intelligent threats.

(**N**) U. S. Government usage: The technical and operational capability of a hostile entity to detect, exploit, or subvert friendly information systems and the demonstrated, presumed, or inferred intent of that entity to conduct such activity.

Définitions du RFC4949

$ **threat**

1a. (**I**) A potential for violation of security, which exists when there is an entity, circumstance, capability, action, or event that could cause harm. (See: dangling threat, INFOCON level, threat action, threat agent, threat consequence. Compare: attack, vulnerability.)

1b. (**N**) Any circumstance or event with the potential to adversely affect a system through unauthorized access, destruction, disclosure, or modification of data, or denial of service. [C4009] (See: sensitive information.)

Usage: (**a**) Frequently misused with the meaning of either "threat action" or "vulnerability". (**b**) In some contexts, "threat" is used more narrowly to refer only to intelligent threats; for example, see definition 2 below. (**c**) In some contexts, "threat" is used more broadly to cover both definition 1 and other concepts, such as in definition 3 below.

Tutorial: A threat is a possible danger that might exploit a vulnerability. Thus, a threat may be intentional or not:
- "Intentional threat": A possibility of an attack by an intelligent entity (e.g., an individual cracker or a criminal organization).
- "Accidental threat": A possibility of human error or omission, unintended equipment malfunction, or natural disaster (e.g., fire, flood, earthquake, windstorm, and other causes listed in [FP031]).

The Common Criteria characterizes a threat in terms of (**a**) a threat agent, (**b**) a presumed method of attack, (**c**) any vulnerabilities that are the foundation for the attack, and (**d**) the system resource that is attacked. That characterization agrees with the definitions in this Glossary (see: diagram under "attack").

2. (**O**) The technical and operational ability of a hostile entity to detect, exploit, or subvert a friendly system and the demonstrated, presumed, or inferred intent of that entity to conduct such activity.

Tutorial: To be likely to launch an attack, an adversary must have (a) a motive to attack, (b) a method or technical ability to make the attack, and (c) an opportunity to appropriately access the targeted system.

3. (**D**) "An indication of an impending undesirable event." [Park]

Deprecated Definition: IDOCs SHOULD NOT use this term with definition 3 because the definition is ambiguous; the definition was intended to include the following three meanings
- "Potential threat": A possible security violation; i.e., the same as definition 1.
- "Active threat": An expression of intent to violate security. (Context usually distinguishes this meaning from the previous one.)
- "Accomplished threat" or "actualized threat": That is, a threat action.

Deprecated Usage: IDOCs SHOULD NOT use the term "threat" with this meaning; instead, use "threat action".

La table des matières de ce document de 365 pages est la suivante:

ftp://ftp.isi.edu/in-notes/rfc4949.txt

RFC4998

Evidence Record Syntax (ERS)

Editée par **T.Gondrom** (Open Text Corporation), **R.Brandner** (InterComponentWare AG) et **U.Pordesch** (Fraunhofer Gesellschaft), cette proposition de standard intitulée '**Evidence Record Syntax**', **ERS** en abrégé, s'intéresse à un problème fondamental à l'ère de l'information numérique et dématérialisée, celui de la création d'une preuve irréfutable, et à long terme, de l'existence d'une donnée, et de manière annexe, de son intégrité.

Il ne s'agit pas ici de remettre en cause les mécanismes de signature existants – lesquels permettent de garantir l'origine et la non altération d'une information et donc l'existence de celle-ci à une date donnée (celle de la signature) – mais de proposer d'y adjoindre un mécanisme complémentaire ayant pour objet d'assurer que cette garantie restera valide sur une très longue période de temps.

L'expérience montre en effet que la durée de vie de nombreux mécanismes de condensation et algorithmes de signature n'est pas infinie, et dans certains cas, bien inférieure à la durée de conservation des données qu'ils protégent. Il apparaît alors difficile de pouvoir maintenir la valeur probante d'une signature, ou de tout autre élément de preuve, sur une très longue période de temps durant laquelle les mécanismes de production originaux peuvent à tout instant être démontrés faibles et les certificats arriver à expiration.

Rappelons qu'en France, la durée de conservation de certains documents est légiférée: 30 ans pour la matière civile et 100 ans pour l'acte authentique, durée pour laquelle devra être assurée la vérification pérenne des signatures accompagnant ces documents.

Deux solutions sont bien souvent envisagées pour résoudre ce problème qui consistent soit à **re-signer** les données après vérification de la signature courante (ce qui revient à remplacer la signature originale) soit à simplement **sur-signer** l'ensemble des informations – données et signature(s) ayant permis de produire une preuve valide à une date donnée. Cependant et même sans être un spécialiste du droit, il est clair que la valeur probante d'un document dont la signature originale aura été remplacée ne sera certainement pas la même que celle de la signature d'un document et de sa signature originale.

Dans le cas présent, les auteurs considèrent que le problème précédent peut être solutionné s'il est possible de prouver que les éléments de preuve existaient avant que l'évènement susceptible de les remettre en cause apparaisse. Ils partent du principe de l'existence d'un service d'horodatage certifié – la norme **ISO 18014** est citée en annexe – lequel permet la création d'éléments de sécurité dits Timestamp permettant de vérifier l'existence d'une donnée à une date et heure donnée. Ce service pourra être utilisé pour générer, lorsque cela sera nécessaire, un certificat horodaté portant sur les données et les éléments de preuve associés précédents.

Encore faut-il s'entendre sur un format unifié autorisant l'archivage de toutes les informations permettant de garantir l'exploitabilité de ces éléments sur le long terme: représentation des certificats, identification des algorithmes utilisés, ...

Le **RFC3126** '**Electronic Signature Formats for long term electronic signatures**' - datant de Septembre 2001 et édité par D.Pinkas, J.Ross et N.Pope - décrit le format d'un élément dénommé '**Archive Timestamp Attribute**' compatible avec le format dit **CMS** (Cryptographic Message Syntax). Le **RFC4998** s'inspire de cette approche en l'étendant pour être compatible avec n'importe quel format de données en tenant compte des pré requis concernant l'archivage de données à long terme décrits dans le **RFC4810** '**Long-Term Archive Service Requirements**'.

Il en résulte une structure de données décrite en syntaxe **ASN.1** et dénommée '**EvidenceRecord**'. Celle-ci est constituée d'une liste de structures référencées '**Archive Timestamps**' et d'informations additionnelles.

```
EvidenceRecord ::= SEQUENCE {
 version                  INTEGER { v1(1) } ,
 digestAlgorithms         SEQUENCE OF AlgorithmIdentifier,
 cryptoInfos              [0] CryptoInfos OPTIONAL,
 encryptionInfo           [1] EncryptionInfo OPTIONAL,
 archiveTimeStampSequence ArchiveTimeStampSequence
}
CryptoInfos ::= SEQUENCE SIZE (1..MAX) OF Attribute
```

Elle pourra être stockée indépendamment des données archivées ou être intégrée à celles-ci sous la forme d'un attribut spcifique. Les processus de génération et de vérification de chacune de ces structures sont par ailleurs détaillés.

La table des matières de ce document de 32 pages est la suivante:

ftp://ftp.isi.edu/in-notes/rfc4998.txt

LES NORMES ISO

UN RAPIDE ETAT DE L'ART : 13335, 17799, 27000, ...

- **Description**

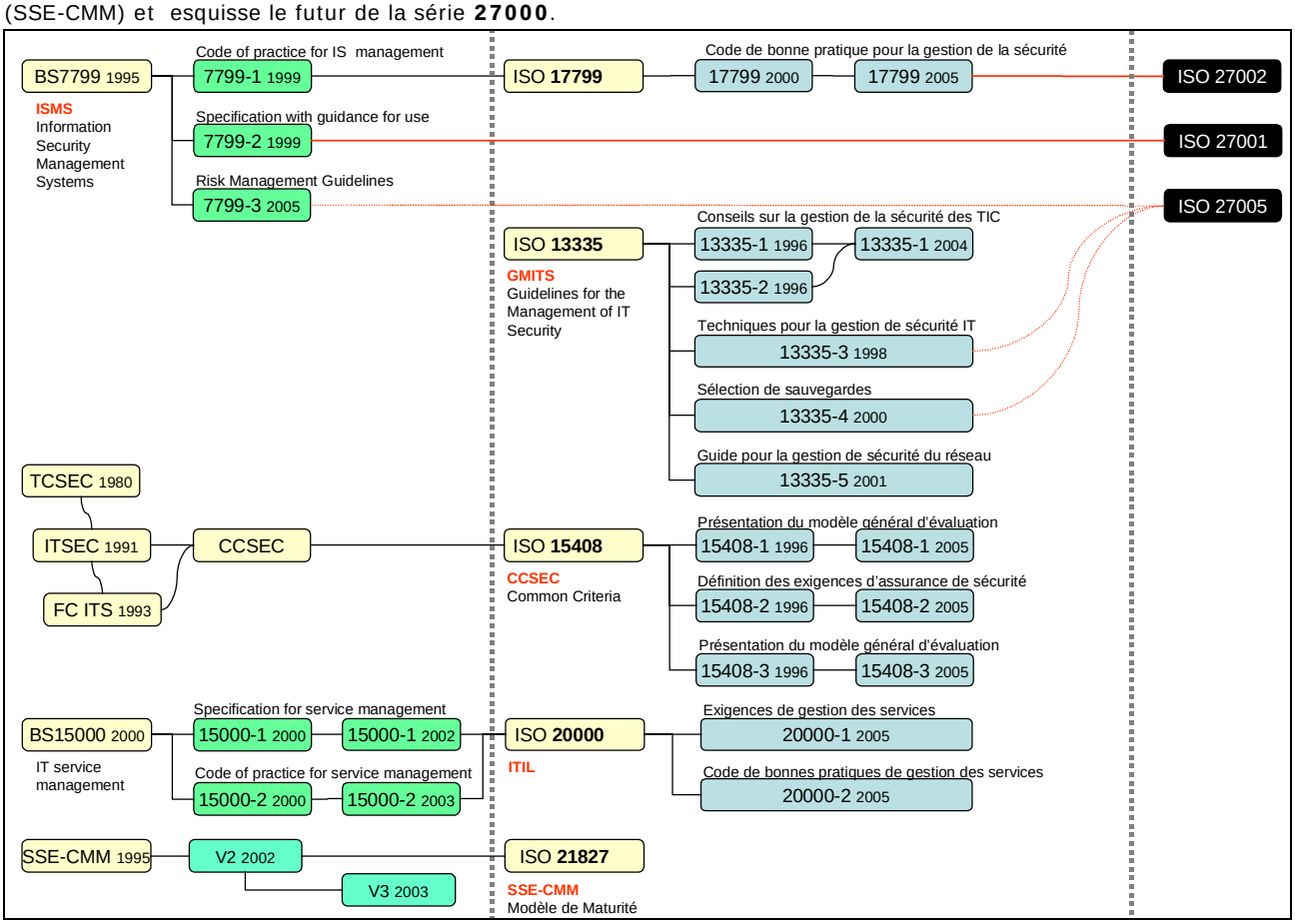
Des normes **ISO** connues de toute personne versée dans sécurité informatique, la famille des normes **ISO 27000** est probablement la norme actuellement la plus médiatisée au point de damner le pion à la norme **ISO 17799** à la une des médias spécialisés il y a encore quelques mois. A l'origine de cet engouement, la volonté de l'ISO de regrouper sous un même chapeau – celui de la famille des normes 27000 - un ensemble jusqu'alors disparate de normes traitant de la gestion de la sécurité des SI.

Que l'on ne s'y trompe pas, cette louable intention ne s'accompagnera pas immédiatement de la disparition des normes ayant fait l'objet de cette opération. Ainsi et à titre d'exemple, la norme ISO 17799:2005 sera probablement toujours accessible (et vendue) sous cette référence quand elle a pourtant été renommée ISO 27002 en 2007.

Cette opération de réorganisation était absolument indispensable, le système de référencement devenant inintelligible au fil du temps. Rappelons que le cycle de vie d'une norme n'est pas aussi simple que l'on pourrait le croire. Ainsi, nombre de normes **ISO** trouvent leurs racines dans une ou plusieurs normes nationales gérées par des instances locales tels l'**AFNOR** pour la France, le **BS** pour l'Angleterre ou encore le **BSI** pour l'Allemagne après une lente maturation. Ajoutons à cela que chaque pays aura à cœur de voir sa norme nationale devenir une norme internationale avec les enjeux économiques associés que l'on imagine et l'on comprendra les dérives constatées vis-à-vis des planifications initialement établies.

Une synthèse de la genèse et de l'évolution des normes susceptibles d'intéresser le responsable d'un système d'information nous apparaît en conséquence être indispensable. Nous avions eu l'occasion de découvrir une telle synthèse il y a quelques années mais n'avons pu retrouver celle-ci pour la mettre à jour. Nous proposons donc à nos lecteurs un synoptique que nous espérons ne pas être trop entaché d'erreurs.

Celui-ci trace l'historique des normes ISO **13335** (GMITS), **15408** (CCSEC), **17799** (ISMS), **20000** (ITIL), **21827** (SSE-CMM) et esquisse le futur de la série **27000**.



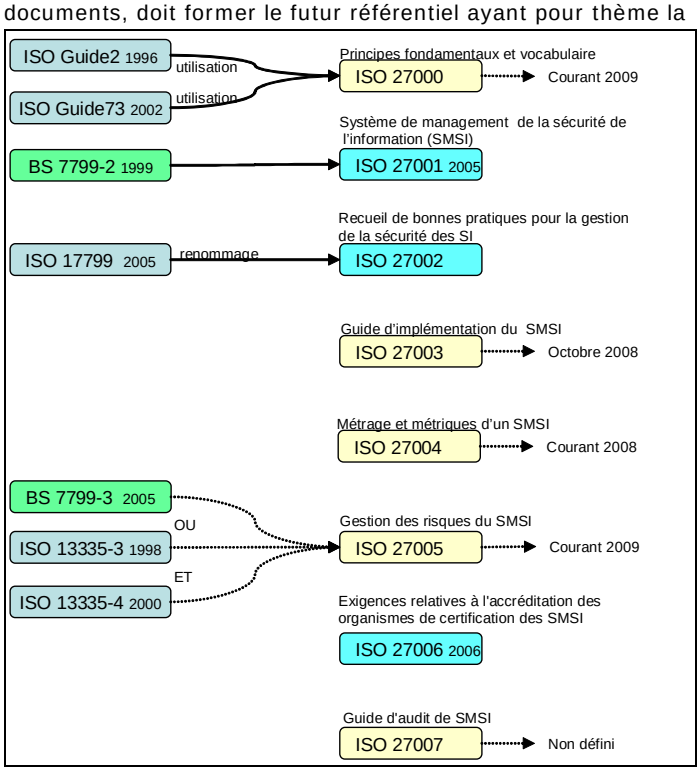
Cette dernière famille, qui pourrait compter plus de 10 documents, doit former le futur référentiel ayant pour thème la gestion de la sécurité des systèmes d'information, le sigle **ISMS** (**I**nformation **S**ecurity **M**anagement **S**ystems) ou **SMSI** (**S**ystème de **M**anagement de la **S**écurité des **I**nformations) en Français attaché à la norme anglaise **BS 7799** étant repris.

Comme on peut le voir sur le diagramme de synthèse ci-contre, cette série de normes est loin d'être finalisée, trois normes seulement étant publiées à ce jour, à savoir:

- la norme **ISO 27001** qui n'est que la reprise de la seconde partie de la norme **BS 7799**,
- la norme **ISO 27002** qui résulte du renommage de la norme **ISO 17799** elle-même inspirée de la première partie de la **BS 7799** et
- la norme **ISO 27006** indispensable car définissant les conditions d'accréditation des organismes chargés de certifier les sociétés en conformité avec la norme **ISO 27001**.

L'**ISO Guide 73** intitulé 'Risk Management – Vocabulary - Guidelines for Use in Standards' sur lequel pourrait s'appuyer la future norme ISO 27000 est en cours de révision par le **TMB** (**T**echnical **M**anagement **B**oard). Ce dernier travaille aussi sur la nouvelle norme **ISO 31000** dédiée à la gestion du risque.

Notre tableau de synthèse est bien loin d'être définitif et devra très certainement faire l'objet de mises à jour dans les mois à venir d'autant que nous



n'avons encore mentionné ni les normes **ISO 15443** 'A framework for IT security assurance' et **ISO 15446** 'Guide on the production of protection profiles and security targets' ni les guides techniques complémentaires dont **ISO 18044** 'Security incident management' ou encore **ISO 18045** 'Methodology for IT security evaluation'.

Pour en revenir à la norme **27001**, qui est à l'assurance sécurité ce qu'est la norme **ISO 9001** à l'assurance qualité, il est important de noter que son **homologation NF** (Norme Française) est en cours.

Le projet **PR NF ISO 27001** (indice de classement Z74-221PR) a ainsi fait l'objet d'une enquête probatoire nationale qui s'est terminée le 20 juillet dernier. L'homologation pourrait alors bien être prononcée avant la fin de l'année.Son application deviendra alors exigible avec les conséquences que cela suppose notamment en terme d'obligations pour certains fournisseurs de service. Dans un éditorial récent, le cabinet **Bensoussan** n'hésite à pas à recommander « de faire référence dès aujourd'hui à cette norme dans les contrats passés avec les prestataires et les sous-traitants pour la rendre obligatoire ».

Il y a fort à parier que les demandes de certification vont exploser d'ici la fin de l'année en notant toutefois qu'à la fin du mois d'Août seules trois sociétés Françaises étaient certifiées au titre de la norme ISO 27001:2005 et deux au titre de la norme BS7799:2002 si l'on se réfère aux données publiées sur le site '**ISO27001Certificates**'. A cette même date, quelques 2323 certificats ISO 27001:2005 avaient attribués dans le monde.

- **Complément d'information**

http://www.iso27001security.com/	- Portail de synthèse
http://www.iso27001certificates.com/	- Etat des certifications 7799/27001
http://www.legifrance.gouv.fr/WAspad/Visu?cid=802056&indice=1&table=JORF&ligneDeb=1	- Annonce enquête AFNOR

ALERTES ET ATTAQUES

ALERTES

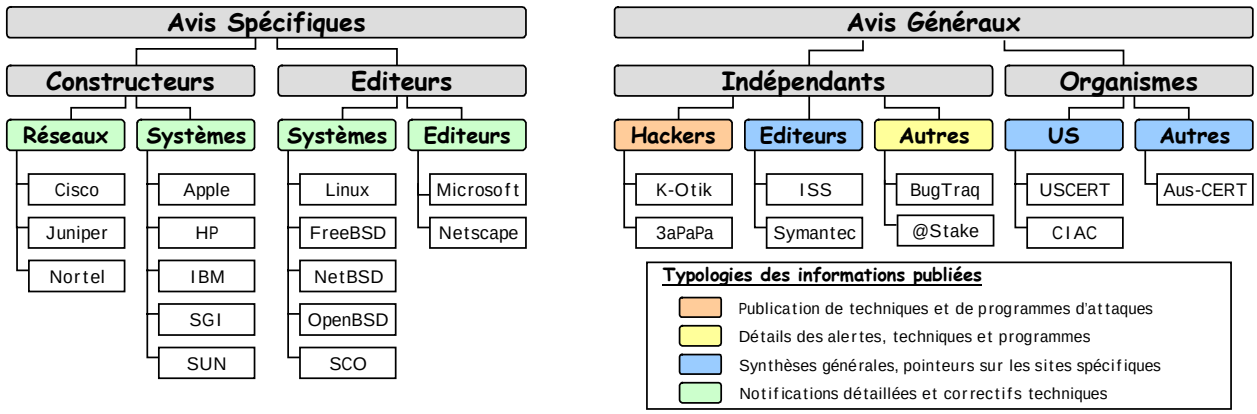
GUIDE DE LECTURE

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 :

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

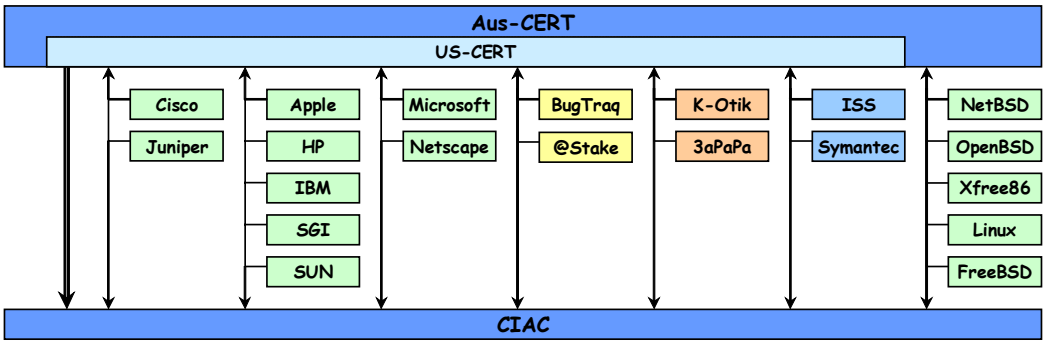
La seconde alternative, pour séduisante quelle soit, ne peut être raisonnablement mise en œuvre étant donné l'actuelle diversité des systèmes impactés. En conséquence, nous nous proposons de maintenir une synthèse des avis classée par organisme émetteur de l'avis.

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 :

- Recherche d'informations générales et de tendances : Lecture des avis du CERT et du CIAC
- Maintenance des systèmes : Lecture des avis constructeurs associés
- 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

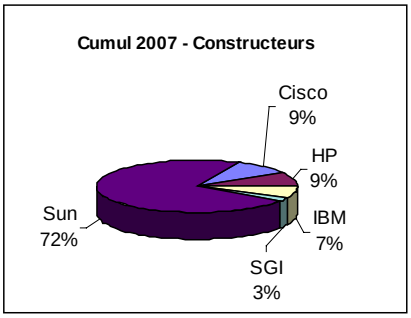
SOURCE
TITRE
Description sommaire
URL pointant sur la source d'information
Référence(s) CVE si définie(s)

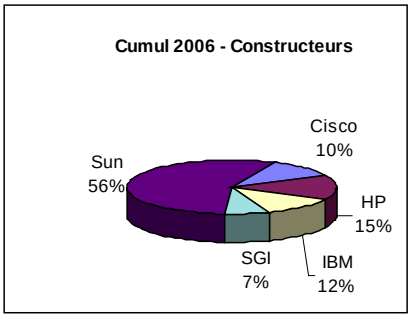
SYNTHESE MENSUELLE

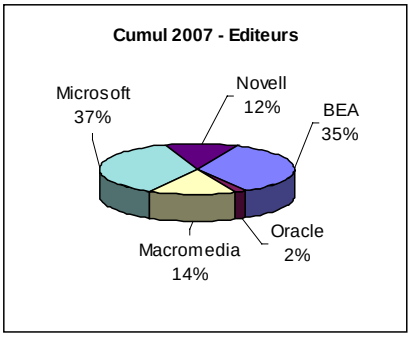
Le tableau suivant propose un récapitulatif du nombre d'avis publiés pour la période courante, l'année en cours et l'année précédente. Ces informations sont mises à jour à la fin de chaque période de veille. L'attention du lecteur est attirée sur le fait que certains avis sont repris et rediffusés par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

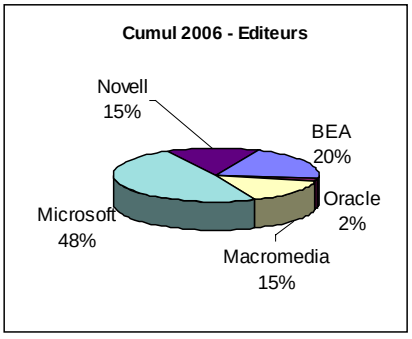
Période du **30/08/2007** au **27/09/2007**

		Cumul	
	Période	2007	2006
Organisme	**21**	**261**	**251**
US-CERT TA	1	32	39
US-CERT ST	2	19	9
CIAC	18	210	203
Constructeurs	**39**	**412**	**324**
Cisco	2	38	34
HP	2	36	49
IBM	2	29	38
SGI	1	11	22
Sun	32	298	181
Editeurs	**6**	**147**	**162**
BEA	0	51	32
Oracle	0	3	4
Macromedia	1	21	24
Microsoft	4	54	78
Novell	1	18	24
Unix libres	**88**	**877**	**994**
Linux RedHat	19	188	151
Linux Fedora	33	288	207
Linux Debian	15	138	311
Linux Mandr.	17	189	225
Linux SuSE	4	66	74
FreeBSD	0	8	26
Autres	**10**	**172**	**111**
iDefense	9	144	80
eEye	1	8	21
NGS Soft.	0	20	10









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.

ADOBE

Faille dans Adobe 'Connect Enterprise Server'			
Un manque de validation dans Adobe 'Connect Enterprise Server' permet d'exposer des informations.			
Forte	11/09	Adobe 'Connect Enterprise Server' version 6	
Correctif existant		Pages visibles	Validation insuffisante des données
Adobe		http://www.adobe.com/support/security/bulletins/apsb07-14.html	
CVE-2007-4651			

ALCATEL/LUCENT

Exécution de commandes dans 'OmniPCX Enterprise'			
Un manque de validation des données permet d'exécuter des commandes arbitraires sur un serveur vulnérable.			
Forte	17/09	Alcatel/Lucent 'OmniPCX Enterprise' version R7.1 et inférieures	
Correctif existant		Script 'masterCGI'	Validation insuffisante des données
Alcatel/Lucent		http://www1.alcatel-lucent.com/psirt/statements/2007002/OXEUMT.htm	
CVE-2007-3010			

APACHE

Contournement de la sécurité dans Apache 'Geronimo'			
Une erreur de conception permet à un attaquant d'obtenir un accès non autorisé à un composant EJB.			
Forte	09/09	Apache 'Geronimo' version 2.0.1, 2.1	
Palliatif proposé		EJB de gestion 'MEJB'	Erreur de conception
Apache		https://issues.apache.org/jira/browse/GERONIMO-3456	
Geronimo		http://geronimo.apache.org/2007/09/07/mejb-security-alert.html	

Déni de service et exécution de code dans 'Struts'			
Une faille permet de provoquer un déni de service ou l'exécution de code arbitraire.			
Forte	18/07	Apache 'Struts' versions inférieures à 2.0.9	
Correctif existant		Fonctionnalité 'altSyntax'	Validation insuffisante des données
Apache Struts		http://struts.apache.org/2.x/docs/s2-001.html	
CVE-2007-4556			

Déni de service via 'mod_proxy'			
Une faille permet de provoquer un déni de service d'un serveur vulnérable.			
Forte	30/08	Apache 'Apache' versions inférieures à 2.2.6-dev	
Correctif existant		Module 'mod_proxy'	Non disponible
Apache		http://httpd.apache.org/security/vulnerabilities_20.html	
Apache		http://httpd.apache.org/security/vulnerabilities_22.html	
CVE-2007-3847			

APPLE

Exécution de code arbitraire dans 'iTunes'			
Un débordement de buffer permet de provoquer l'exécution de code arbitraire.			
Forte	06/09	Apple 'iTunes' versions inférieures à 7.4	
Correctif existant		Gestion des couvertures	Débordement de buffer
Apple		http://lists.apple.com/archives/security-announce/2007/Sep/msg00000.html	
CVE-2007-3752			

AVAYA

Exécution de code via des contrôles ActiveX Avaya			
Des débordements de buffer permettent d'exécuter du code arbitraire sur une machine vulnérable.			
Forte	18/09	Avaya 'IP Softphone' version R5.2, R6.0	
Correctif existant		Contrôles ActiveX	Débordement de buffer
Avaya		http://support.avaya.com/elmodocs2/security/ASA-2007-314.htm	
CVE-2007-3286			

BACKUP MANAGER

Exposition d'informations via 'Backup Manager'

Une erreur de conception permet d'exposer des informations sensibles à un utilisateur local.

Moyenne	03/09	Backup Manager 'Backup Manager' versions inférieures à 0.6.3	
Correctif existant		Crédences 'FTP'	Erreur de conception
Debian Bug report		http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=439392	

CA

Multiples failles dans les produits ARCserve Backup

Des multiples failles permettent de provoquer l'exécution de code et de commandes avec des droits privilégiés.

Forte	20/09	'ARCServe Backup for Laptops and Desktops' versions r4.0 à r11.5, 'Desktop Management Suite' versions 11.0 à 11.2, 'Protection Suites' version r2	
Correctif existant		Gestionnaire de commandes	Erreur de conception, Débordements d'entier, de buffer
CA		http://supportconnectw.ca.com/public/sams/lifeguard/infodocs/caarcservebld-securitynotice.asp	
CVE-2007-5003, CVE-2007-5004, CVE-2007-5005, CVE-2007-5006			

CISCO

Prise de contrôle des produits Cisco Video Surveillance

Des erreurs de conception permettent à un attaquant de prendre le contrôle à distance d'un équipement.

Critique	05/09	'Cisco Video Surveillance SP/ISP Gateway Encoder/Decoder'	
Correctif existant		Authentification 'Telnet'	Erreur de conception
Cisco		http://www.cisco.com/warp/public/707/cisco-sa-20070905-video.shtml	

Contournement de la sécurité dans des produits Cisco

Une faille permet à un attaquant de contourner des listes de contrôle d'accès afin d'atteindre un équipement.

Moyenne	26/09	Cisco '7600 series', 'Catalyst 6500 series'	
Correctif existant		IP 'loopback' (127.0.0.0/8)	Erreur de conception
Cisco		http://www.cisco.com/warp/public/707/cisco-sr-20070926-lb.shtml	

Contournement de l'authentification 'VTY'

Sous certaines conditions, une erreur de configuration permet à un attaquant de contourner l'authentification 'VTY'.

Forte	29/08	Cisco 'IOS' version 12.2E, 12.2F, 12.2S	
Correctif existant		Authentification 'VTY'	Erreur de configuration
Cisco		http://www.cisco.com/warp/public/707/cisco-sr-20070829-vty.shtml	

Déni de service des produits Cisco 'CSM' et 'CSM-S'

Deux failles permettent de provoquer des dénis de service de ces équipements.

Forte	05/09	Cisco 'CSM' et 'CSM-S'	
Correctif existant		Paquet 'TCP' de 'out of order'	Non disponible
Cisco		http://www.cisco.com/warp/public/707/cisco-sa-20070905-csm.shtml	

Déni de service via le moteur d'expression régulière

Un débordement de pile dans Cisco 'IOS' permet de provoquer un redémarrage d'un équipement vulnérable.

Moyenne	12/09	Cisco 'IOS' versions 12.0 à 12.4	
Aucun correctif		Moteur d'expression régulière	Débordement de pile
Cisco		http://www.cisco.com/warp/public/707/cisco-sr-20070912-regexp.shtml	

Exposition d'informations Cisco 'ASA'

Une faille dans Cisco 'Adaptive Security Appliance' ('ASA') permet d'exposer des informations sensibles.

Moyenne	05/09	Cisco 'Adaptive Security Appliance'	
Correctif existant		Fonctionnalité 'AAA'	Erreur de conception
Us-CERT		http://www.kb.cert.org/vuls/id/563673	

CLAROLINE

Multiples failles dans 'Claroline'

Plusieurs failles permettent de mener des attaques "XSS", d'obtenir des informations ou d'exécuter du code.

Forte	04/09	Claroline 'Claroline' versions inférieures à 1.8.6	
Correctif existant		Scripts divers	Validation insuffisante des données
Claroline		http://www.claroline.net/wiki/index.php/Changelog_1.8.x#Security	

ELINKS

Interception de données dans 'elinks'

Une faille non documentée permet à un attaquant distant d'intercepter des données sensibles.

Forte	25/09	ELinks 'elinks' version 0.11.3	
Aucun correctif		Requête 'POST'	Non disponible
Red Hat		http://www.redhat.com/archives/fedora-package-announce/2007-September/msg00335.html	
CVE-2007-5034			

FETCHMAIL

Déni de service de 'fetchmail'			
Un déréférencement de pointeur NULL dans 'fetchmail' permet de provoquer un déni de service du produit.			
Moyenne	30/08	Fetchmail 'fetchmail' versions inférieures à 6.3.9	
Correctif existant		Gestion des messages d'erreur	Déréférencement de pointeur NULL
Fetchmail		http://fetchmail.berlios.de/fetchmail-SA-2007-02.txt	
CVE-2007-4565			

GALLERY

Vulnérabilités dans 'gallery'			
Des failles non documentées affectent le produit 'gallery'.			
N/A	05/09	Gallery 'gallery' versions inférieures à 2.2.3	
Correctif existant		Modules 'WebDAV' et 'Reupload'	Non disponible
Gallery		http://gallery.menalto.com/gallery_2.2.3_released	

GFORGE

Injection SQL dans 'Gforge'			
Un manque de validation permet à un attaquant distant d'injecter des commandes SQL arbitraires.			
Forte	07/09	GForge 'Gforge' versions inférieures à 3.1	
Aucun correctif		Non disponible	Manque de validataion
Debian		http://lists.debian.org/debian-security-announce/debian-security-announce-2007/msg00133.html	
CVE-2007-3913			

GNOME

Exécution de code arbitraire dans 'Balsa'			
Un débordement de pile dans le client de messagerie 'Balsa' permet d'exécuter du code arbitraire.			
Forte	24/09	Gnome 'Balsa' versions inférieures à 2.3.20	
Correctif existant		Fonction 'ir_fetch_seq()'	Débordement de pile
Gnome bugzilla		http://bugzilla.gnome.org/show_bug.cgi?id=474366	

GNU

Déni de service dans 'tar'			
Une faille non documentée permet de provoquer un déni de service du produit.			
Moyenne	03/09	Gnu 'tar' version non disponible	
Aucun correctif		Fonction 'safer_name_suffix()'	Non disponible
SuSE		http://www.novell.com/linux/security/advisories/2007_18_sr.html	
CVE-2007-4476			

HP

Accès distants non autorisés via 'logins'			
Une faille permet à un attaquant distant d'obtenir un accès non autorisé à un système vulnérable.			
Critique	18/09	HP 'HP-UX' version B.11.11, B.11.23, B.11.31	
Correctif existant		Commande 'logins'	Erreur de conception
HP		http://www4.itrc.hp.com/service/cki/docDisplay.do?admit=-938907319+1190186285577+28353475&docId=emr_na-c01167886-1	

Réduction du niveau de sécurité dans HP 'SHM'			
Une faille permet de réduire le niveau de sécurité par l'installation incomplète du produit 'OpenSSL'.			
Moyenne	10/09	HP 'System Management Homepage'	
Correctif existant		'OpenSSL'	Non disponible
HP		http://www4.itrc.hp.com/service/cki/docDisplay.do?admit=-938907319+1190010388309+28353475&docId=emr_na-c01164065-1	

IBM

Corruption d'informations dans 'Rational ClearQuest'			
Une faille non documentée permet de corrompre des données de la base sous-jacente au produit.			
Faible	24/09	IBM 'Rational ClearQuest' versions 7.0 à 7.0.1, 2002, 2003	
Correctif existant		Non disponible	Non disponible
IBM		http://www-1.ibm.com/support/docview.wss?uid=swg21268116	

Multiples failles dans le client Tivoli Storage Manager			
Des failles permettent de provoquer l'exécution de code et un déni de service, et d'obtenir des informations.			
Forte	20/09	IBM 'Tivoli Storage Manager' versions 5.1 à 5.4	
Aucun correctif		Divers	Débordement de buffer
IBM		http://www-1.ibm.com/support/docview.wss?uid=swg21268775	

Multiples vulnérabilités dans IBM 'AIX'			
De multiples failles permettent de provoquer un déni de service du système ou l'exécution de code arbitraire.			
Forte	05/09	IBM 'AIX' version 5.2, version 5.3	
Correctif existant		Commandes diverses	Débordement de buffer
AusCERT		http://www.auscert.org.au/render.html?it=8052	

Faille non documentée dans WebSphere Application Server			
Une faille non documentée affecte un composant du serveur 'WebSphere Application Server'.			
N/A	10/09	IBM 'WebSphere Application Server' versions inférieures à 6.1.0.11	
Correctif existant		Composant 'Edge'	Non disponible
IBM		http://www-1.ibm.com/support/docview.wss?uid=swg27007951	

KDE

Accès non autorisé via 'KDM'			
Un utilisateur local peut obtenir un accès non autorisé avec des droits privilégiés à l'aide de 'KDM'.			
Moyenne	20/09	KDE 'KDE' versions 3.3.0 à 3.5.7	
Correctif existant		Application 'KDM'	Erreur de conception
KDE		http://www.kde.org/info/security/advisory-20070919-1.txt	
CVE-2007-4569			

LINUX

Déni de service du noyau Linux			
Une faille dans le code 'ptrace' du noyau Linux permet de provoquer un déni de service.			
Forte	25/09	Linux 'Noyau 2.6' versions 2.6.20 et 2.6.21	
Correctif existant		Fonctionnalité 'ptrace'	Déréférencement de pointeur NULL
Kernel.org		http://bugzilla.kernel.org/show_bug.cgi?id=8765	
Secunia		http://secunia.com/advisories/26935/	
CVE-2007-3731			

Elévation de privilèges dans le noyau Linux			
Une erreur de codage sur plate-forme 64 bits permet à un utilisateur d'élever ses privilèges.			
Moyenne	24/09	Linux 'Noyau 2.4' versions inférieures à 2.4.35.3, 'Noyau 2.6' versions inférieures à 2.6.22.7	
Correctif existant		IA32 system call emulation	Erreur de codage
Kernel.org		http://www.kernel.org/pub/linux/kernel/v2.4/ChangeLog-2.4.35.3	
Kernel.org		http://www.kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.22.7	
CVE-2007-4573			

Déni de service dans le noyau Linux			
Une faille dans un pilote du noyau Linux 2.6 permet de provoquer un déni de service du sous-système USB.			
Moyenne	31/08	Linux 'Noyau 2.6' versions inférieures à 2.6.22.6	
Correctif existant		Pilote 'pwc'	Erreur de conception
SecurityFocus		http://www.securityfocus.com/bid/25504	
Kernel.org		http://www.kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.22.6	

Multiples vulnérabilités dans le noyau Linux			
Deux failles permettent de provoquer un déni de service du noyau ou d'obtenir des droits privilégiés.			
Moyenne	14/09	Linux 'Noyau' version non disponible	
Aucun correctif		Architecture 'PowerPC'	Erreur de codage
Red Hat Bugzilla		https://bugzilla.redhat.com/show_bug.cgi?id=253313	
Red Hat Bugzilla		https://bugzilla.redhat.com/show_bug.cgi?id=253314	
CVE-2007-3739, CVE-2007-3740			

MARSHAL

Corruption de fichiers via les produits MailMarshal			
Des attaques de type traversée de répertoire permettent de corrompre des fichiers et d'exécuter du code.			
Moyenne	30/08	Marshal 'MailMarshal Exchange' version 5.x, 'MailMarshal SMTP' versions 5.5, 6.x, 2006	
Correctif existant		Archives de type 'TAR'	Traversée de répertoire
Marshal		http://marshal.com/kb/article.aspx?id=11780	

MICROSOFT

Exécution de code arbitraire dans Microsoft 'Agent'			
Un débordement de pile permet à un attaquant distant d'exécuter du code arbitraire sur un poste vulnérable.			
Critique	11/09	Microsoft 'Windows 2000' version SP4	
Correctif existant		Contrôle Microsoft 'Agent'	Débordement de pile
Microsoft		http://www.microsoft.com/technet/security/Bulletin/MS07-051.mspx	
CVE-2007-3040			

Elévation de privilèges dans Windows Services for UNIX			
Une faille permet à un utilisateur local d'élever ses privilèges.			
Forte	11/09	Microsoft 'Subsystem for UNIX-based Applications', 'Windows Services for UNIX' versions 3.0 et 3.5.	
Correctif existant		Fichiers binaires avec 'setuid'	Non disponible
Microsoft		http://www.microsoft.com/technet/security/Bulletin/MS07-053.mspx	
CVE-2007-3036			

Exécution de code dans 'MSN Messenger'			
Un débordement de tas permet de provoquer l'exécution de code arbitraire sur un poste vulnérable.			
Forte	11/09	'MSN Messenger' version 6.2, 7.0, 7.5, 'Windows Live Messenger' version 8.0	
Correctif existant		Sessions Video et webcam	Débordement de tas
Microsoft		http://www.microsoft.com/technet/security/Bulletin/MS07-054.mspx	
CVE-2007-2931			

Faille dans 'Crystal Reports' pour 'Visual Studio'			
Un débordement de buffer dans 'Crystal Reports' pour 'Visual Studio' permet d'exécuter du code arbitraire.			
Forte	11/09	Microsoft 'Visual Studio' version 2005, SP1, 2002 SP1, 2003, 2003 SP1	
Correctif existant		Gestion des fichiers '.RPT'	Débordement de pile
Microsoft		http://www.microsoft.com/technet/security/Bulletin/MS07-052.mspx	
CVE-2006-6133			
Full-Disclosure		http://lists.grok.org.uk/pipermail/full-disclosure/2007-September/065798.html	

MIT

Exécution de code arbitraire dans 'Kerberos 5'			
Deux failles dans 'Kerberos 5' permettent de provoquer l'exécution de code arbitraire sur un serveur vulnérable.			
Forte	04/09	MIT 'Kerberos 5' versions 1.4 à 1.6.2	
Correctif existant		Démon 'kadmind'	Débordement de pile, Erreur de codage
MIT		http://web.mit.edu/kerberos/www/advisories/MITKRB5-SA-2007-006.txt	
CVE-2007-3999, CVE-2007-4000			

MOZILLA

Exécution de code arbiraire via des fichiers QuickTime			
Une faille autorise un attaquant distant à exécuter du code arbitraire sur un poste vulnérable.			
Critique	18/09	Mozilla 'Firefox' version 2.0.0.6 et inférieures, 'SeaMonkey' toute versions	
Correctif existant		Fichiers 'QuickTime Media-Link',	Erreur de conception
Mozilla		http://www.mozilla.org/security/announce/2007/mfsa2007-28.html	
CVE-2006-4965			

NETBSD

Déni de service via le pilote d'affichage			
Un débordement de buffer permet de provoquer un déni de service d'une plate-forme vulnérable.			
Forte	13/09	NetBSD 'NetBSD' versions 3.0 à 4.0 Beta2	
Correctif existant		Pilote d'affichage	Débordement de buffer
NetBSD		http://archives.neohapsis.com/archives/netbsd/2007-q3/0035.html	
CVE-2007-3654			

NOVELL

Contournement de la sécurité des produits Novell			
Une erreur de conception dans Novell 'iChain', 'BorderManager' et 'Access Management' permet de contourner la sécurité offerte par ces produits.			
Forte	07/09	Novell 'Access Management' version 3, 'BorderManager' version 3.8, 'iChain' version 2.3	
Correctif existant		Encodage	Erreur de conception
Novell		https://secure-support.novell.com/KanisaPlatform/Publishing/539/3193302_f.SAL_Public.html	

OPENOFFICE.ORG

Exécution de code dans 'OpenOffice'			
Des débordements de buffer permettent de provoquer l'exécution de code avec les droits de l'utilisateur courant.			
Forte	17/09	OpenOffice.org 'OpenOffice' versions inférieures à 2.3	
Correctif existant		Images de type 'TIFF'	Débordement de buffer
OpenOffice.org		http://www.openoffice.org/security/cves/CVE-2007-2834.html	
CVE-2007-2834			

OPENSSH

Contournement de l'authentification dans 'OpenSSH'

Une faille dans 'OpenSSH' permet à un attaquant distant de contourner l'authentification à l'aide d'un cookie 'X11'.

Forte	04/09	OpenSSH 'OpenSSH' versions inférieures à 4.7	
Correctif existant		Gestion des cookies 'X11'	Erreur de conception
OpenSSH		http://www.openssh.com/txt/release-4.7	
CVE-2007-4752			

PHP

Multiples vulnérabilités dans 'PHP'

De multiples failles permettent de provoquer, entre autres choses, des dénis de service et l'exécution de code.

Forte	03/09	PHP 'PHP' versions inférieures à 5.2.4	
Correctif existant		Diverses fonctions	Multiples failles
PHP		http://www.php.net/releases/5_2_4.php	
CVE-2007-2872, CVE-2007-3378, CVE-2007-3806			

QUAGGA

Multiples failles dans 'Quagga'

De multiples failles non documentées dans 'Quagga' permettent de provoquer des dénis de service de l'application.

Forte	07/09	Quagga 'Quagga' versions inférieures à 0.99.9	
Correctif existant		Non disponible	Non disponible
Quagga		http://www.quagga.net/download/quagga-0.99.9.changelog.txt	

RED HAT

Vulnérabilité dans le paquetage 'aide'

Une faille dans le paquetage 'aide' permet de contourner la sécurité offerte par le produit.

Moyenne	05/09	Red Hat 'Red Hat Enterprise Linux' , 'Red Hat Enterprise Linux Desktop' version 5(client)	
Correctif existant		Paquetage 'aide'	Erreur de configuration
Red Hat		http://rhn.redhat.com/errata/RHSA-2007-0539.html	
CVE-2007-3849			

SAMBA

Elévation de privilèges via 'Samba'

Une erreur de codage dans 'Samba' permet à un utilisateur Windows d'élever ses privilèges.

Forte	12/09	Samba 'Samba' versions 3.0.25 à 3.0.25c	
Correctif existant		Bibliothèque 'idmap_ad.so'	Erreur de codage
Samba		http://www.samba.org/samba/security/CVE-2007-4138.html	
CVE-2007-4138			

SUN

Déni de service dans 'Sun Solaris'

Une faille non documentée dans Sun 'Solaris' permet à un utilisateur local de provoquer un déni de service.

Forte	26/09	Sun 'Solaris' version 8, 9, 10	
Aucun correctif		Noyau 'Solaris'	Non disponible
Sun		http://sunsolve.sun.com/search/document.do?assetkey=1-26-103084-1&searchclause=	

Déni de service de Sun 'Solaris'

Une faille dans un pilote de Sun 'Solaris' permet de provoquer un déni de service du système.

Forte	25/09	Sun 'Solaris' version 8, 9, 10	
Correctif existant		Pilote 'HID'	Non disponible
Sun		http://sunsolve.sun.com/search/document.do?assetkey=1-26-102883-1	

Déni de service via 'SPECFS'

Une faille permet à un utilisateur local de provoquer un déni de service du système.

Forte	31/08	Sun 'Solaris' version 8, 9, 10	
Correctif existant		Système de fichiers	Non disponible
Sun		http://sunsolve.sun.com/search/document.do?assetkey=1-26-103009-1	

TROLLTECH

Déni de service via 'Qt'

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

Moyenne	03/09	Trolltech 'Qt' version 3.x, 4.x	
Correctif existant		'QUtf8Decoder::toUnicode()'	Débordement de buffer
Trolltech		http://trolltech.com/company/newsroom/announcements/press.2007-09-03.7564032119	
CVE-2007-4137			

WEBMIN

Exécution de commandes arbitraires via 'Webmin'			
Une faille permet de provoquer une exécution de commandes arbitraires sur un poste Windows vulnérable.			
Forte	24/09	Webmin 'Webmin' versions inférieures à 1.370	
Correctif existant		Paramètres dans une URL	Non disponible
Webmin		http://www.webmin.com/security.html	

YAHOO!

Exécution de code arbitraire dans 'Yahoo! Messenger'			
Des débordements de buffer permettent d'exécuter du code arbitraire sur un poste vulnérable.			
Forte	30/08	Yahoo! 'Yahoo! Messenger' version 8.1	
Correctif existant		Contrôle 'YVerInfo.GetInfo.1'	Débordement de buffer
Yahoo!		http://messenger.yahoo.com/security_update.php?id=082907	
CVE-2007-4515			

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.

ADOBE

Exécution de code arbitraire via 'Reader'			
Une faille non documentée dans Adobe 'Reader' permet d'exécuter du code arbitraire sur une machine vulnérable.			
Forte	20/09	Adobe 'Reader' version 8.1	
Aucun correctif		Non disponible	Non disponible
SecurityTracker		http://securitytracker.com/id?1018723	

AOL

Exécution de code dans 'AOL Instant Messenger'			
Une faille non documentée permet d'exécuter du code arbitraire sur un poste vulnérable.			
Forte	14/09	AOL 'AOL Instant Messenger' version 6.1.41.2	
Aucun correctif		Fenêtre de notification	Non disponible
SecurityFocus		http://www.securityfocus.com/bid/25659	

APACHE

"Cross-Site Scripting" dans 'Tomcat'			
Une faille permet à un attaquant de mener des attaques de type "Cross-Site Scirpting".			
Forte	06/09	Apache 'Tomcat' version 4.1.31	
Correctif existant		Application 'calendar.jsp'	Erreur de validation
FullDisclosure		http://lists.grok.org.uk/pipermail/full-disclosure/2007-September/065598.html	
CVE-2006-7196			

"Cross-Site Scripting" via le module 'mod_autoindex'			
Une faille du serveur 'Apache' permet de mener des attaques de type "Cross-Site Scripting".			
Forte	12/09	Apache 'Apache' version 2.2.4 et inférieures	
Correctif existant		Module 'mod_autoindex'	Erreur de codage
SecurityReason		http://securityreason.com/achievement_securityalert/46	
CVE-2007-4465			

APPLE

Exécution de commandes arbitraires via 'QuickTime'			
Une faille pour les navigateurs permet de provoquer l'exécution de commandes arbitraires.			
Forte	12/09	Apple 'QuickTime' version non disponible	
Aucun correctif		Greffons pour les navigateurs	Erreur de conception
Gnucitizen		http://www.gnucitizen.org/blog/0day-quicktime-pwns-firefox	

Déni de service de 'Safari'			
Un débordement de buffer dans Apple 'Safari' permet de provoquer un déni de service.			
Forte	08/09	Apple 'Safari' version 3.0.3	
Aucun correctif		Non disponible	Débordement de buffer
Bugtraq		http://marc.info/?l=bugtraq&m=118918307832347&w=2	

AXIS

Multiples failles dans le produit Axis '207W'

De multiples failles permettent de provoquer un déni de service et à mener des attaques de type "XSS" ou "CRSF".

Forte	15/09	AXIS '207W'	
Aucun correctif		Interface Web de gestion	Multiples problèmes
Bugtraq		http://marc.info/?l=bugtraq&m=118987784821192&w=2	

BARRACUDA NETWORKS

"Cross-Site Scripting" dans 'Barracuda Spam Firewall'

Un attaquant distant peut exploiter un manque de validation afin de mener des attaques de "Cross-Site Scripting".

Forte	21/09	Barracuda Networks 'Barracuda Spam Firewall' version 3.4.10.102	
Correctif existant		Console Web d'administration	Validation insuffisante des données en entrée
Bugtraq		http://www.securityfocus.com/archive/1/480238/30/30/threaded	

CA

Failles dans 'BrightStor Hierarchical Storage Manager'

De multiples failles permettent de provoquer l'exécution de code arbitraire.

Forte	26/09	CA 'BrightStor Hierarchical Storage Manager' version r11.5	
Correctif existant		Service 'CsAgent'	Débordement de buffer
Full-Disclosure		http://lists.grok.org.uk/pipermail/full-disclosure/2007-September/066118.html	
CVE-2007-5082, CVE-2007-5083, CVE-2007-5084			

ENTERPRISEDB

Exécution de code dans 'EnterpriseDB Advanced Server'

Une erreur de conception permet de provoquer un déni de service ou l'exécution de code arbitraire.

Moyenne	04/09	EnterpriseDB 'EnterpriseDB Advanced Server' version 8.2	
Correctif existant		Fonctions de déboguage	Erreur de conception
SecurityFocus		http://www.securityfocus.com/bid/25481	
Bugtraq		http://www.securityfocus.com/archive/1/478057	

ER MAPPER

Exécution de code arbitraire dans 'ER Mapper'

Un débordement de buffer permet à un attaquant distant d'exécuter du code et de générer un déni de service.

Forte	18/09	ER Mapper 'Earth Resource Mapping' versions inférieures à 3.4.0.242	
Aucun correctif		Contrôle ActiveX 'NCSView'	Débordement de buffer
SecurityFocus		http://www.securityfocus.com/bid/25584	
CVE-2007-4470			

FCRON

Corruption de fichiers arbitraires dans 'Fcron'

Un utilisateur peut exploiter une faille afin de corrompre des fichiers à l'aide d'une attaque par lien symbolique.

Moyenne	18/09	Fcron 'Fcron' version 2.9.5, version 3.0	
Aucun correctif		Fichiers temporaires	Traversée de répertoire
SecurityFocus		http://www.securityfocus.com/bid/25693	
CVE-2006-0575			

FIREBIRD

Dénis de service dans 'Firebird'

De multiples failles dans le produit 'Firebird' permettent à un attaquant de générer des dénis de service.

Forte	30/08	Firebird 'Firebird' versions inférieures à 2.0.2	
Correctif existant		Divers	Erreur de conception
Secunia		http://secunia.com/advisories/26615	
CVE-2007-5007			

GNU

Exécution de code arbitraire dans 'QGit'

Une faille permet à un attaquant local d'écrire sur des fichiers existants et d'exécuter du code arbitraire.

Forte	11/09	Gnu 'QGit' version 1.5.6	
Aucun correctif		Fonction 'DataLoader::doStart'	Erreur de conception
Bugzilla		https://bugzilla.redhat.com/show_bug.cgi?id=268381	
CVE-2007-4631			

GOOGLE

"Cross-Site Scripting" dans les équipements Google			
Un manque de validation permet de mener des attaques de type "Cross-Site Scripting".			
Forte	26/09	Google 'Search Application'	
Aucun correctif		Non disponible	Validation insuffisante des données
CPNI		http://www.cpni.gov.uk/Products/3402.aspx	

HP

Déni de service via le contrôle ActiveX 'hpqutil.dll'			
Un débordement de tas dans le contrôle ActiveX 'hpqutil.dll' de HP permet de provoquer un déni de service.			
Forte	14/09	HP 'All-in-One Series Web Release', 'Photo and Image Gallery' version 1.1	
Aucun correctif		Contrôle ActiveX 'hpqutil.dll'	Débordement de tas
Bugtraq		http://www.securityfocus.com/archive/1/479442	
SecurityFocus		http://www.securityfocus.com/bid/25673	

IBM

Débordement de buffer dans 'DB2 Universal Database'			
Un débordement de buffer autorise un attaquant à prendre le contrôle de la base.			
Forte	31/08	IBM 'DB2 Universal Database' version 9.1 Fixpack 2	
Correctif existant		Fonction dédiée	Débordement de buffer
Full Disclosure		http://lists.grok.org.uk/pipermail/full-disclosure/2007-August/065543.html	

ID3LIB

Elévation de privilèges dans 'id3lib'			
Une faille dans le produit 'id3lib' permet à un utilisateur local d'obtenir une élévation de privilèges.			
Moyenne	11/09	id3lib 'id3lib' version 3.8.3	
Aucun correctif		Fonction 'RenderV2ToFile()'	Erreur de conception
SecurityTracker		http://www.securitytracker.com/alerts/2007/Sep/1018667.html	
CVE-2007-4460			

IMAGEMAGICK

Multiples failles dans la bibliothèque 'ImageMagick'			
De multiples failles permettent de provoquer des dénis de service et l'exécution de code arbitraire.			
Forte	19/09	ImageMagick 'ImageMagick' version 6.3.4	
Correctif existant		Fonctions diverses	Erreur de codage, Débordements de buffer, d'entier
iDefense		http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=594	
iDefense		http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=595	
iDefense		http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=596	
iDefense		http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=597	
CVE-2007-4985, CVE-2007-4986, CVE-2007-4987, CVE-2007-4988			

INVISION

"Cross-Site Scripting" dans 'Invision Power Board'			
Une faille permet à un attaquant de modifier des privilèges d'utilisateurs ou de mener des attaques "XSS".			
Forte	13/09	Invision 'Invision Power Board' version 2.3.1 et inférieures	
Correctif existant		Données en entrée	Manque de validation des données
SecurityFocus		http://www.securityfocus.com/bid/25656	

JFFNMS

Multiples failles dans 'JFFNMS'			
De multiples failles permettent de mener des attaques "XSS, d'injecter du code SQL, et d'obtenir des informations.			
Forte	12/09	JFFNMS 'JFFNMS' version 0.8.3-pre2, version 0.8.3-pre1	
Correctif existant		Script 'auth.php'	Manque de validation
Secunia		http://secunia.com/advisories/25587	
CVE-2007-3189, CVE-2007-3190, CVE-2007-3191, CVE-2007-3192, CVE-2007-3204			

KASPERSKY LAB

Déni de service via les produits Kaspersky			
Une faille permet de provoquer un déni de service d'une plate-forme vulnérable.			
Forte	24/09	'Kaspersky Antivirus' versions 6.x et 7.x, 'Kaspersky Internet Security' versions 6.x et 7.x	
Aucun correctif		Pilote 'klif.sys'	Erreur de conception
Rootkit.com		http://www.rootkit.com/newsread.php?newsid=778	

KTORRENT

Ecrasement de fichier dans 'KTorrent'			
Une faille permet à un attaquant d'effectuer une traversée de répertoire et d'écraser des fichiers de façon arbitraire.			
Forte	12/09	KTorrent 'KTorrent' versions inférieures à 2.1.3	
Correctif existant		Fichier 'torrent.cpp'	Traversée de répertoire
SecurityFocus		http://www.securityfocus.com/bid/23745	
CVE-2007-1799			

LIBSNDFILE

Exécution de code arbitraire via 'libsndfile'			
Un débordement de buffer permet d'exécuter du code arbitraire dans les applications utilisant cette bibliothèque.			
Forte	21/09	libsndfile 'libsndfile' version 1.0.17	
Aucun correctif		Fichier 'flac.c'	Débordement de buffer
SecurityFocus		http://www.securityfocus.com/bid/25758	
CVE-2007-4974			

LIGHTTPD

Exécution de code arbitraire via 'mod_fastcgi'			
Un débordement de buffer dans un module du serveur Web 'Lighttpd' permet d'exécuter du code arbitraire.			
Forte	10/09	Lighttpd 'Lighttpd' version 1.4.17 et inférieures	
Correctif existant		Module 'mod_fastcgi'	Débordement de buffer
SECWEB		http://secweb.se/en/advisories/lighttpd-fastcgi-remote-vulnerability/	
CVE-2007-4727			

LINUX

Exposition d'informations dans le noyau Linux			
Une erreur de codage permet d'exposer localement des informations provenant du noyau.			
Moyenne	25/09	Linux 'Noyau 2.6' version 2.6.22.1	
Correctif existant		Pilote 'ALSA'	Erreur de codage
iDefense		http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=600	
CVE-2007-4571			

MAPSERVER

"Cross-Site Scripting" dans 'MapServer'			
De multiples failles permettent de mener des attaques de type "Cross-Site Scripting" et d'exécuter du code.			
Forte	24/08	MapServer 'MapServer' versions inférieures à 4.10.3	
Correctif existant		Fonctions diverses	Débordement de buffer, Manque de validation
Secunia		http://secunia.com/advisories/26561	
CVE-2007-4629			

MEDIAWIKI

"Cross-Site Scripting" dans 'MediaWiki'			
Une faille dans le produit 'MediaWiki' permet à un attaquant de mener des attaques de type "Cross-Site Scripting".			
Forte	19/09	MediaWiki 'MediaWiki' version 1.11.0rc1 et inférieures	
Correctif existant		Mode impression	Nettoyage des paramètres en entrée
Secunia		http://secunia.com/advisories/26772	
CVE-2007-4828, CVE-2007-4883			

MERAK

"Cross-Site Scripting" dans 'Merak Mail Server'			
Un manque de validation autorise un attaquant distant à mener des attaques de type "Cross-Site Scripting".			
Forte	18/09	Merak 'Merak Mail Server' version 8.9.1 et 8.9.2	
Correctif existant		Contenu des courriers	Validation insuffisante des données
MWR InfoSecurity		http://www.mwrinfosecurity.com/publications/mwri_merak-webmail-xss-advisory_2008-09-17.pdf	

MICROSOFT

Déni de service dans Microsoft 'Visual FoxPro'			
Une faille permet à un attaquant distant d'exécuter du code arbitraire et de générer un déni de service.			
Forte	07/09	Microsoft 'Visual FoxPro ' version 6.0	
Aucun correctif		Contrôle activeX 'fpole.ocx'	Débordement de buffer
SecurityFocus		http://www.securityfocus.com/bid/25571	

Déni de service via un ActiveX 'SQL Server'			
Un débordement de buffer permet de provoquer un déni de service d'un poste vulnérable ou d'exécuter du code.			
Forte	07/09	Microsoft 'SQL Server' version 2005 SP2	
Aucun correctif		Contrôle 'SQLDMO.SQLServer'	Débordement de buffer
SecurityFocus		http://www.securityfocus.com/bid/25594	

Contournement de la sécurité via Windows Media Player			
Une faille permet d'afficher une page Web avec des droits privilégié.			
Forte	18/09	Microsoft 'Windows XP' version SP2	
Aucun correctif		Lecteur 'Windows Media Player',	Erreur de conception
Gnucitizen		http://www.gnucitizen.org/blog/backdooring-windows-media-files	

Corruption de fichiers via l'ActiveX 'VBTOVSI.DLL'			
Une faille dans le contrôle ActiveX 'VBTOVSI.DLL' de Microsoft permet de corrompre des fichiers arbitraires.			
Forte	11/09	Microsoft 'VB To VSI Support Library' version 1.0	
Aucun correctif		Contrôle 'VBTOVSI.DLL',	Erreur de conception
SecurityFocus		http://www.securityfocus.com/bid/25635	

Débordement de buffer dans 'Visual Basic'			
Un débordement de buffer dans 'Visual Basic' permet d'exécuter du code arbitraire.			
Forte	11/09	Microsoft 'Visual Basic' version 6.0	
Aucun correctif		'VBP_Open'	Débordement de buffer
SecurityFocus		http://www.securityfocus.com/bid/25629	

Déni de service dans l'explorateur Windows			
Un débordement de buffer permet à un attaquant de provoquer un déni de service.			
Forte	27/09	Microsoft 'Windows Server 2003', 'Windows Vista', 'Windows XP'	
Aucun correctif		Image 'PNG'	Débordement de buffer
SecurityFocus		http://www.securityfocus.com/bid/25816	

Déni de service dans Microsoft 'Process Monitor'			
Une faille permet à un attaquant de provoquer un déni de service.			
Forte	19/09	Microsoft 'Process Monitor ' version 1.22	
Aucun correctif		Non disponible	Non disponible
SecurityFocus		http://www.securityfocus.com/bid/25719	

Déni de service dans Microsoft 'RegMon'			
Une faille non documentée dans le produit 'RegMon' permet à un attaquant de provoquer un déni de service.			
Forte	19/09	Microsoft 'RegMon' version 7.04	
Aucun correctif		Non disponible	Non disponible
SecurityFocus		http://www.securityfocus.com/bid/25721	

Déni de service de 'Windows Live Messenger'			
Un débordement de buffer permet de provoquer un déni de service ou l'exécution potentielle de code arbitraire.			
Forte	24/09	Microsoft 'Windows Live Messenger' version 8.1	
Aucun correctif		Bibliothèque 'ole32.dll'	Débordement de buffer
SecurityFocus		http://www.securityfocus.com/bid/25795	

Exposition d'informations dans 'ISA Server'			
Une faille dans Microsoft 'ISA Server' permet à un attaquant distant d'obtenir des informations.			
Forte	20/09	Microsoft 'ISA Server' version 2004	
Correctif existant		Serveur mandataire 'SOCKS4'	Erreur de conception
Zero Day Init.		http://www.zerodayinitiative.com/advisories/ZDI-07-053.html	
CVE-2007-4991			

Multiples failles dans 'Visual Studio'			
De multiples failles dans 'Visual Studio' permettent d'exécuter des commandes arbitraires, entre autres choses.			
Forte	11/09	Microsoft 'Visual Studio' version 6.0	
Aucun correctif		Contrôle ActiveX 'PDWizard.ocx'	Non disponible
SecurityFocus		http://www.securityfocus.com/bid/25638	

Débordement de tas dans la classe 'FileFind'			
Une classe de Microsoft 'Foundation Class Library' est vulnérable à un débordement de tas.			
N/A	14/09	Microsoft 'Foundation Class Library' version 8.0	
Aucun correctif		Classe 'FindFile'	Débordement de tas

MOZILLA

Contournement de sécurité dans 'Bugzilla'			
Une faille dans le produit 'Bugzilla' permet à un attaquant de créer des comptes et de contourner la sécurité.			
Forte	20/09	Mozilla 'Bugzilla' version 3.1.1 et inférieures	
Correctif existant		'offer_account_by_email()'	Manque de validation du paramètre 'createemailregexp'
Bugzilla		http://www.bugzilla.org/security/3.0.1/	

Injection de commandes arbitraires via 'Firefox'			
Une faille permet d'injecter et d'exécuter des commandes arbitraires sur un poste Windows vulnérable.			
Forte	06/09	Mozilla 'Firefox' version 2.0.0.6	
Aucun correctif		'mailto', 'nntp', 'news' et 'snews'	Non disponible
SecurityFocus		http://www.securityfocus.com/bid/25543	

MPLAYER

Exécution de code arbitraire dans 'MPlayer'			
Un débordement de tas permet de provoquer l'exécution de code arbitraire ou un déni de service.			
Forte	13/09	MPlayer 'MPlayer' version 1.0-rc1	
Aucun correctif		Fichier 'aviheader.c'	Débordement de tas
SecurityFocus		http://www.securityfocus.com/bid/25648	

NORMAN

Exécution de code arbitraire dans Norman Virus Control			
Une faille dans le produit 'Norman Virus Control' permet à un utilisateur local d'exécuter du code arbitraire.			
Forte	31/08	Norman 'Norman Virus Control' version 5.82	
Aucun correctif		Pilote 'nvcoaft51'	Erreur de conception
milw0rm		http://www.milw0rm.com/exploits/4345	

PHP

Déni de service via la fonction 'iconv_substr()'			
Une faille non documentée dans 'PHP' permet de provoquer un déni de service de l'application.			
Moyenne	05/09	PHP 'PHP' version 5.2.4 et inférieures	
Aucun correctif		Fonction 'iconv_substr()'	Non disponible
Bugtraq		http://marc.info/?l=bugtraq&m=118902402918450&w=2	

Dénis de service dans 'PHP'			
Des failles non documentées dans 'PHP' permettent de provoquer des dénis de service de l'application.			
Moyenne	06/09	PHP 'PHP' version 5.2.4 et inférieures	
Aucun correctif		Fonctions 'iconv()'	Non disponible
Bugtraq		http://marc.info/?l=bugtraq&m=118910559111743&w=2	

PHPBB

Inclusion arbitraire de fichiers dans 'phpBB2'			
Une faille dans le produit 'phpBB2' permet à un attaquant d'inclure des fichiers de façon arbitraire.			
Forte	24/09	phpBB 'phpBB2' version 1.53a	
Correctif existant		Paramètre 'phpbb_root_path'	Manque de validation
Secunia		http://secunia.com/advisories/26888/	

PHPWIKI

Multiples failles dans 'PhpWiki'			
De multiples failles permettent d'exécuter du code PHP et de contourner les mécanismes d'authentification.			
Forte	11/09	PhpWiki 'PhpWiki' versions inférieures à 1.3.13p1	
Correctif existant		Page 'index.php/UpLoad'	Manque de validation, Erreur de conception
Secunia		http://secunia.com/advisories/25595	
CVE-2007-2024, CVE-2007-2025, CVE-2007-3193			

PYTHON

Corruption de fichiers via 'Python'			
Une faille permet à un attaquant d'effectuer une traversée de répertoire et de corrompre des fichiers de façon.			
Forte	31/08	Python 'Python' version 2.5	
Aucun correctif		Validation de données	Traversée de répertoire
Secunia		http://secunia.com/advisories/26623	
CVE-2007-4559			

Exécution de code ou déni de service dans 'Python'			
Des débordements d'entier permettent de provoquer l'exécution de code ou un déni de service de l'application.			
Forte	17/09	Python 'Python' versions 1.5.2 à 2.5.1	
Aucun correctif		Module 'ImageOP'	Débordement d'entier
SecurityFocus		http://www.securityfocus.com/bid/25696	

QUIKSOFT

Déni de service dans Quiksoft 'EasyMail'			
Un débordement de buffer dans Quiksoft 'EasyMail' permet à un attaquant distant de générer un déni de service.			
Forte	03/09	Quiksoft 'EasyMail Objects' version 6.0.1	
Aucun correctif		Contrôle ActiveX 'emsmtp.dll'	Débordement de buffer
SecurityFocus		http://www.securityfocus.com/bid/25467	

REAL NETWORKS

Déni de service de 'RealPlayer' et 'Helix Player'			
Une division par zéro permet de provoquer un déni de service de ces lecteurs multimédia.			
Forte	11/09	Real Networks 'Helix Player' version 1.0.6, 'RealPlayer' version 10.1, 10.0.9, 10.5-GOLD	
Aucun correctif		Gestion des fichiers '.au'	Division par zéro
SecurityFocus		http://www.securityfocus.com/bid/25627	

RSA SECURITY

"Cross-Site Scripting" dans 'enVision Platform'			
Une faille dans RSA Security 'enVision Platform' permet de mener des attaques de type "Cross-Site Scripting".			
Forte	12/09	RSA Security 'enVision Platform' version 3.3.6 Build 0115	
Aucun correctif		Non disponible	Validation insuffisante des données
SecurityFocus		http://www.securityfocus.com/bid/25645	

SKK

Déni de service dans 'SKK Tools'			
Une faille dans le produit 'SKK Tools' permet à un utilisateur local de provoquer un déni de service.			
Forte	21/09	SKK 'SKK Tools ' version 1.2	
Aucun correctif		Fichiers temporaires	Création de liens symboliques, écrasement de fichiers
SecurityFocus		http://www.securityfocus.com/bid/25739	
CVE-2007-3916			

SOPHOS

Contournement de sécurité dans 'Sophos'			
Une erreur de conception permet à un attaquant de contourner la sécurité via des fichiers d'archives corrompus.			
Forte	07/09	Sophos 'Sophos Anti-Virus' versions inférieures à 2.49.0	
Correctif existant		Fichier d'archives malformés	Erreur de conception
Secunia		http://secunia.com/advisories/26726/	

"Cross-Site Scripting" via 'Sophos Anti-Virus'			
Un manque de validation dans 'Sophos Anti-Virus' permet de mener des attaques de type "Cross-Site Scripting".			
Forte	06/09	Sophos 'Sophos Anti-Virus' version 6.5.4 R2	
Correctif existant		Gestion des archives 'ZIP'	Validation insuffisante des données
Full Disclosure		http://lists.grok.org.uk/pipermail/full-disclosure/2007-September/065609.html	
CVE-2007-4512			

SUN

Débordement de buffer dans 'Sun Java Web Start'			
Un débordement de buffer dans 'Sun Java Web Start' permet à un attaquant de provoquer un déni de service.			
Moyenne	20/09	Sun 'Sun Java Web Start' version 1.6.0	
Aucun correctif		'Sun Java Web Start'	Débordement de buffer
SecurityFocus		http://www.securityfocus.com/bid/25734	

TREND MICRO

Exécution de code arbitraire dans 'ServerProtect'			
Un débordement de pile dans une fonction de 'ServerProtect' permet de provoquer l'exécution de code arbitraire.			
Forte	07/09	Trend Micro 'ServerProtect' version 5.58	
Correctif existant		Bibliothèque 'TMReg.dll'	Débordement de pile
Zero Day Init.		http://www.zerodayinitiative.com/advisories/ZDI-07-051.html	
CVE-2007-4731			

UNIX

Vulnérabilité dans 'NFS'			
Une faille non documentée et aux conséquences inconnues affecte 'NFS'.			
N/A	03/09	Unix 'NFS' version 4	
Aucun correctif		Translation 'name' vers 'uid'	Non disponible
SuSE		http://www.novell.com/linux/security/advisories/2007_18_sr.html	
CVE-2007-4135			

VMWARE

Multiples vulnérabilités dans les produits VMware			
De multiples failles permettent de provoquer l'exécution de code, des DOS et une élévation de privilèges.			
Forte	19/09	Se référer à l'avis original	
Correctif existant		Serveur 'DHCP'	Corruption de la mémoire
Full-Disclosure		http://lists.grok.org.uk/pipermail/full-disclosure/2007-September/065902.html	
CVE-2007-0061, CVE-2007-0062, CVE-2007-0063, CVE-2007-4496, CVE-2007-4497			

WINSCP

Téléchargements arbitraires de fichiers dans 'WinSCP'			
Une faille permet à un attaquant de télécharger ou de déposer des fichiers arbitraires sur une machine vulnérable.			
Moyenne	13/09	WinSCP 'WinSCP' versions inférieures à 4.0.4	
Correctif existant		Protocoles 'scp://' et 'sftp://'	Non disponible
SecurityFocus		http://www.securityfocus.com/bid/25655	

WIRESHARK

Déni de service via le dissecteur 'DNP3'			
Une faille dans un dissecteur de 'Wireshark' (Ethereal) permet de provoquer un déni de service du produit.			
Moyenne	30/08	Wireshark 'Wireshark' versions inférieures à 0.99.6	
Correctif existant		Dissecteur 'DNP3'	Non disponible
SecurityTracker		http://securitytracker.com/id?1018635	

WORDPRESS

"Cross-Site Scripting" dans 'WordPress'			
Une faille dans le produit 'WordPress' permet à un attaquant de mener des attaques de type "Cross-Site Scripting".			
Forte	12/09	WordPress 'WordPress' versions inférieures à 2.2.3	
Correctif existant		Données en entrée	Manque de validation
Secunia		http://www.securityfocus.com/bid/25639	

"Cross-Site Scripting" dans 'WordPress'			
Une faille dans le produit 'WordPress' permet à un attaquant de mener des attaques de types "Cross-Site Scripting".			
Forte	24/09	WordPress 'WordPress ' version 2.0	
Aucun correctif		'user_login' et 'user_email'	Manque de validation
SecurityFocus		http://www.securityfocus.com/bid/25769	

X.ORG

Elévation de privilèges dans 'X.org'			
Un débordement de buffer dans 'X.org' permet à un attaquant d'élever ses privilèges.			
Forte	10/09	X.Org 'X.org' versions inférieures à 1.4	
Correctif existant		Extension 'composite'	Débordement de buffer
Secunia		http://secunia.com/advisories/26743/	
CVE-2007-4730			

YAHOO!

Exécution de code arbitraire dans 'Yahoo! Messenger'			
Une faille peut être exploitée pour exécuter du code arbitraire sur un système via une page HTML.			
Forte	20/09	Yahoo! 'Yahoo! Messenger' version 8.1.0.421	
Aucun correctif		Méthode 'GetFile()'	Non disponible
SecurityTracker		http://www.securitytracker.com/alerts/2007/Sep/1018715.html	

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:

APACHE

Nouvelles versions du serveur Web 'Apache'

Les versions 1.3.39, 2.0.61 et 2.2.6 du serveur Web 'Apache' ont été publiées. Elles corrigent de multiples failles dans le serveur et plusieurs modules qui permettent de provoquer des dénis de service, l'exposition d'informations et autorisent de mener des attaques de type "Cross-Site Scripting".

http://www.apache.org/dist/httpd/CHANGES_1.3.39

http://www.apache.org/dist/httpd/CHANGES_2.2.6 http://www.apache.org/dist/httpd/CHANGES_2.0.61

CVE-2006-5752, CVE-2007-1862, CVE-2007-1863, CVE-2007-3304, CVE-2007-3847

CA

Correctifs pour 'BrightStor ARCserve Backup'

CA a annoncé la disponibilité de correctifs pour 'BrightStor ARCserve Backup Laptop & Desktop' qui est vulnérables à de multiples débordements de buffer. Ces failles permettent de provoquer l'exécution de code arbitraire. La référence CVE CVE-2007-3216 a été attribuée.

http://supportconnectw.ca.com/public/sams/lifeguard/infodocs/caarcservebld-securitynotice.asp

CVE-2007-3216

CIAC

Reprise de l'alerte Cisco 97819

Le CIAC a repris, sous la référence R-342, l'alerte Cisco 97819 concernant des erreurs de conception dans les produits Cisco 'Video Surveillance' qui permettent à un attaquant de prendre le contrôle à distance.

http://www.ciac.org/ciac/bulletins/r-342.shtml

Reprise de l'alerte Cisco 97826

Le CIAC a repris, sous la référence R-351, l'alerte Cisco 97826 concernant deux failles dans Cisco 'CSM' (Content Switching Modules) et 'CSM-S' (Content Switching Module with SSL) qui permettent de provoquer des dénis de service de ces équipements.

http://www.ciac.org/ciac/bulletins/r-351.shtml

Reprise de l'alerte Debian DSA-1361

Le CIAC a repris, sous la référence R-338, l'alerte Debian DSA-1361 concernant un débordement de buffer dans le produit 'policyd' qui permet à un attaquant via l'envoi de nombreuses commandes SMTP de créer un déni de service.

http://www.ciac.org/ciac/bulletins/r-338.shtml

CVE-2007-3791

Reprise de l'alerte Debian DSA-1366

Le CIAC a repris, sous la référence R-345, l'alerte Debian DSA-1366 concernant la disponibilité de correctifs pour 'clamav' sous Debian GNU/Linux version 3.1 (sarge) et 4.0 (etch) qui corrigent des failles dans l'anti-virus 'ClamAV' qui permettent d'exécuter du code arbitraire et de provoquer des dénis de service du produit.

http://www.ciac.org/ciac/bulletins/r-345.shtml

CVE-2007-4510, CVE-2007-4560

Reprise de l'alerte Debian DSA-1367

Le CIAC a repris, sous la référence R-346, l'alerte Debian DSA-1367 concernant la disponibilité de correctifs pour 'krb5' sous Debian GNU/Linux version 3.1 (sarge) et 4.0 (etch) qui corrigent un débordement de buffer dans la bibliothèque RPC qui permet à un attaquant d'exécuter du code arbitraire.

http://www.ciac.org/ciac/bulletins/r-346.shtml

CVE-2007-3999

Reprise de l'alerte Debian DSA-1371

Le CIAC a repris, sous la référence R-353, l'alerte Debian DSA-1371 concernant la disponibilité de correctifs pour 'phpwiki' sous Debian GNU/Linux version 4.0 (etch) qui corrigent de multiples failles dans le produit 'PhpWiki' qui permettent à un attaquant d'exécuter du code PHP arbitraire et de contourner les mécanismes d'authentification.

http://www.ciac.org/ciac/bulletins/r-353.shtml

CVE-2007-2024, CVE-2007-2025, CVE-2007-3193

Reprise de l'alerte Debian DSA-1372

Le CIAC a repris, sous la référence R-347, l'alerte Debian DSA-1372 concernant la disponibilité de correctifs pour 'xorg-server' sous Debian GNU/Linux version 3.1 (sarge) et 4.0 (etch) qui corrigent un débordement de buffer dans 'X.org' qui permet à un attaquant d'élever ses privilèges.

http://www.ciac.org/ciac/bulletins/r-347.shtml

CVE-2007-4730

Reprise de l'alerte Debian DSA-1376

Le CIAC a repris, sous la référence R-358, l'alerte Debian DSA-1376 concernant la disponibilité de correctifs pour le paquetage 'kdebase' sur Debian GNU/Linux version 4.0 (etch). Ils corrigent une faille qui, sous certaines conditions, permet à un utilisateur local d'obtenir un accès non autorisé avec des droits privilégiés à l'aide de 'KDM'.

http://www.ciac.org/ciac/bulletins/r-358.shtml

CVE-2007-4569

Reprise de l'alerte HP HPSBUX02259 (SSRT071439)

Le CIAC a repris, sous la référence R-357, l'alerte HP HPSBUX02259 (SSRT071439) concernant une faille dans la commande 'logins' de 'HP-UX' qui permet à un attaquant distant d'obtenir un accès non autorisé à un système vulnérable.

http://www.ciac.org/ciac/bulletins/r-357.shtml

Reprise de l'alerte Microsoft MS07-051

Le CIAC a repris, sous la référence R-340, l'alerte Microsoft MS07-051 concernant un débordement de pile dans Microsoft 'Agent' qui permet à un attaquant distant d'exécuter du code arbitraire sur un poste vulnérable.

http://www.ciac.org/ciac/bulletins/r-340.shtml

CVE-2007-3040

Reprise de l'alerte Microsoft MS07-052

Le CIAC a repris, sous la référence R-341, l'alerte Microsoft MS07-052 concernant un débordement de buffer dans 'Crystal Reports' pour 'Visual Studio' qui permet d'exécuter du code arbitraire.

http://www.ciac.org/ciac/bulletins/r-341.shtml

CVE-2006-6133

Reprise de l'alerte Microsoft MS07-053

Le CIAC a repris, sous la référence R-344, l'alerte Microsoft MS07-053 concernant une faille non documentée dans les produits 'Windows Services for UNIX' et 'Subsystem for UNIX-based Applications' qui permet à un utilisateur local d'élever ses privilèges.

http://www.ciac.org/ciac/bulletins/r-344.shtml

CVE-2007-3036

Reprise de l'alerte Microsoft MS07-054

Le CIAC a repris, sous la référence R-343, l'alerte Microsoft MS07-054 concernant une faille dans le flux de conversation vidéo qui permet à un attaquant distant d'exécuter du code arbitraire.

http://www.ciac.org/ciac/bulletins/r-343.shtml

CVE-2007-2931

Reprise de l'alerte Red Hat RHSA-2007:0705

Le CIAC a repris, sous la référence R-348, l'alerte Red Hat RHSA-2007:0705 concernant la disponibilité de correctifs pour le noyau Linux des plate-formes Red Hat Enterprise Linux version 5 (server) et Red Hat Enterprise Linux Desktop version 5 (client) qui corrigent de multiples failles qui permettent de provoquer des dénis de service, d'exécuter du code arbitraire ou d'élever ses privilèges, entre autres choses.

http://www.ciac.org/ciac/bulletins/r-348.shtml

CVE-2007-1217, CVE-2007-2875, CVE-2007-2876, CVE-2007-2878, CVE-2007-3739, CVE-2007-3740, CVE-2007-3843, CVE-2007-3851

Reprise de l'alerte Red Hat RHSA-2007:0848

Le CIAC a repris, sous la référence R-356, l'alerte Red Hat RHSA-2007:0848 concernant la disponibilité de correctifs pour le paquetage 'openoffice.org' sur Red Hat Desktop versions 3 et 4, Red Hat Enterprise Linux AS, ES et WS versions 3 et 4, RHEL Optional Productivity Applications version 5 (server), et Red Hat Enterprise Linux Desktop version 5 (client). Ils corrigent des débordements de buffer dans la gestion des images de type 'TIFF' qui permettent de provoquer l'exécution de code arbitraire.

http://www.ciac.org/ciac/bulletins/r-356.shtml

CVE-200-2834

Reprise de l'alerte Red Hat RHSA-2007:0883

Le CIAC a repris, sous la référence R-350, l'alerte Red Hat RHSA-2007:0883 concernant la disponibilité de correctifs pour le paquetage 'qt' sur Red Hat Desktop versions 3 et 4, Red Hat Enterprise Linux AS, ES et WS versions 2.1, 3 et 4, Red Hat Linux Advanced Workstation version 2.1 pour le processeur Itanium, RHEL Desktop Workstation version 5 (client), Red Hat Enterprise Linux version 5 (server), et Red Hat Enterprise Linux Desktop version 5 (client). Ils corrigent deux failles qui permettent de provoquer un déni de service ou une exécution potentielle de code arbitraire.

http://www.ciac.org/ciac/bulletins/r-350.shtml

CVE-2007-0242, CVE-2007-4137

Reprise de l'alerte Red Hat RHSA-2007:0890

Le CIAC a repris, sous la référence R-355, l'alerte Red Hat RHSA-2007:0890 concernant la disponibilité de correctifs pour le paquetage 'php' sur Red Hat Desktop version 4, Red Hat Enterprise Linux AS, ES et WS version 4, RHEL Desktop Workstation version 5 (client), et Red Hat Enterprise Linux version 5 (server). Ils corrigent de multiples failles qui permettent de provoquer des dénis de service entre autres choses.

http://www.ciac.org/ciac/bulletins/r-355.shtml

CVE-2007-2756, CVE-2007-2872, CVE-2007-3799, CVE-2007-3996, CVE-2007-3998, CVE-2007-4658, CVE-2007-4670

Reprise de l'alerte US-CERT VU#281977

Le CIAC a repris, sous la référence R-339, l'avis US-CERT VU#281977 concernant un débordement de buffer dans Quiksoft 'EasyMail' qui permet à un attaquant distant de générer un déni de service.

http://www.ciac.org/ciac/bulletins/r-339.shtml

Reprise de l'alerte US-CERT VU#563673

Le CIAC a repris, sous la référence R-352, l'alerte US-CERT VU#563673 concernant une faille dans Cisco 'Adaptive Security Appliance' ('ASA') qui permet d'exposer des informations sensibles.

http://www.ciac.org/ciac/bulletins/r-352.shtml

Reprise de l'alerte US-CERT VU#589188

Le CIAC a repris, sous la référence R-354, l'alerte US-CERT VU#589188 concernant un débordement de buffer dans le produit 'Earth Resource Mapper' qui permet à un attaquant distant d'exécuter du code arbitraire et de générer un déni de service.

http://www.ciac.org/ciac/bulletins/r-354.shtml

CVE-2007-4470

Reprise de l'alerte US-CERT VU#751808

Le CIAC a repris, sous la référence R-349, l'alerte US-CERT VU#751808 concernant une faille dans les greffons 'QuickTime' pour les navigateurs qui permet de provoquer l'exécution de commandes arbitraires.

http://www.ciac.org/ciac/bulletins/r-349.shtml

Reprise de l'avis Cisco 96082

Le CIAC a repris, sous la référence R-336, l'avis Cisco 96082 concernant un manque de validation dans les produits 'Cisco CallManager' et 'Cisco Communications Manager' qui autorise un attaquant distant à mener des attaques de type "Cross-Site Scripting" et à injecter du code SQL arbitraire dans la base de données sous-jacente.

http://www.ciac.org/ciac/bulletins/r-336.shtml

Reprise de l'avis HP HPSBMA02236 (SSRT061260)

Le CIAC a repris, sous la référence R-337, l'avis HP HPSBMA02236 (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/r-337.shtml

CVE-2007-3872

CISCO

Révision du bulletin 91923

Cisco a révisé le bulletin 91923 concernant des failles dans le produit 'Cisco VPN Client' pour plate-forme Windows qui permettent à un utilisateur local malveillant d'obtenir des privilèges élevés. Cette révision met à jour certaines informations dont les parades.

http://www.cisco.com/warp/public/707/cisco-sa-20070815-vpnclient.shtml

Révision du bulletin 96082

Cisco a révisé le bulletin 96082 (cisco-sa-20070829-ccm) concernant un manque de validation dans les produits 'Cisco CallManager' et 'Cisco Communications Manager' qui autorise un attaquant distant à mener des attaques de type "Cross-Site Scripting" et à injecter du code SQL arbitraire dans la base de données sous-jacente. Cette révision annonce la mise à jour de la section "Exploitation and Public Announcements".

http://www.cisco.com/warp/public/707/cisco-sa-20070829-ccm.shtml

Révision du bulletin 98766

Cisco a révisé le bulletin 98766 concernant un débordement de pile dans le moteur d'expression régulière de Cisco 'IOS'. Cette faille permet de provoquer un déni de service d'un équipement vulnérable. Cette révision met à jour certaines informations dont la liste des opérateurs déclenchant la vulnérabilité.

http://www.cisco.com/warp/public/707/cisco-sr-20070912-regexp.shtml

Révision du bulletin Cisco 98589

Cisco a révisé le bulletin 98589 concernant une erreur de configuration dans 'IOS' qui, sous certaines conditions, permet à un attaquant de contourner l'authentification 'VTY'. Cette révision annonce la mise à jour du tableau des versions vulnérables.

http://www.cisco.com/warp/public/707/cisco-sr-20070829-vty.shtml

HP

Correctifs 'BIND' pour 'OpenVMS'

HP a annoncé, dans le bulletin HPSBOV02261 (SSRT071449), la disponibilité de correctifs pour 'BIND' sur 'TCP/IP Services for OpenVMS Alpha' versions 5.4 à 5.6 et 'TCP/IP Services for OpenVMS I64' versions 5.5 et 5.6. Ils corrigent une faille dans le serveur 'DNS' 'BIND' qui permet de provoquer la corruption du cache.

http://www4.itrc.hp.com/service/cki/docDisplay.do?admit=-938907319+1190620812614+28353475&docId=emr_na-c01174368-1

CVE-2007-2926

Faille Microsoft MS07-051 dans HP 'SMA'

HP a annoncé, dans le bulletin HPSBST02260 (SSRT071471), la vulnérabilité de 'Storage Management Appliance' I, II et III ('SMA') à la faille Microsoft MS07-051 qui permet d'exécuter du code arbitraire sur une machine vulnérable. HP préconise d'installer le correctif Microsoft disponible.

http://www4.itrc.hp.com/service/cki/docDisplay.do?docId=emr_na-c01172326-1

CVE-2007-3040

Révision du bulletin HPSBUX02153 (SSRT061181)

HP a révisé le bulletin HPSBUX02153 (SSRT061181) concernant de multiples failles dans 'Firefox' fourni sur 'HP-UX' versions B.11.11 et B.11.23. Ces failles pouvaient entraîner des dénis de service, des élévations de privilèges et des accès non autorisés. Cette révision annonce la disponibilité de la version 2.0.0.6 de 'Firefox' pour les plate-formes listées.

http://www4.itrc.hp.com/service/cki/docDisplay.do?admit=-938907319+1190186287770+28353475&docId=emr_na-c00771742-6

Révision du bulletin HPSBUX02156 (SSRT061236)

HP a révisé le bulletin HPSBUX02156 (SSRT061236) concernant de multiples failles dans 'Thunderbird' sur 'HP-UX' versions B.11.11 et B.11.23. Elles peuvent entraîner, entre autres choses, l'exécution de code arbitraire et des dénis de service. Cette révision annonce la vulnérabilité de la version B.11.31 de 'HP-UX', ainsi que de la disponibilité du correctif associé.

http://www4.itrc.hp.com/service/cki/docDisplay.do?docId=c00774579

CVE-2006-0292, CVE-2006-0293, CVE-2006-0294, CVE-2006-0295, CVE-2006-0296, CVE-2006-0297, CVE-2006-0298, CVE-2006-0299, CVE-2006-0748, CVE-2006-1045, CVE-2006-1724, CVE-2006-1726, CVE-2006-1727, CVE-2006-1728, CVE-2006-1730, CVE-2006-2775, CVE-2006-2776, CVE-2006-2778, CVE-2006-2779, CVE-2006-2780, CVE-2006-2781, CVE-2006-2783, CVE-2006-2786, CVE-2006-2787, CVE-2006-3113, CVE-2006-3801, CVE-2006-3802, CVE-2006-3803, CVE-2006-3804, CVE-2006-3805, CVE-2006-3806, CVE-2006-3807, CVE-2006-3808, CVE-2006-3809, CVE-2006-3810, CVE-2006-3811

IBM

Correctifs pour IBM 'TCIM'

IBM a annoncé, dans le bulletin 1268889, la vulnérabilité de la base de données Oracle fournie avec 'Tivoli Compliance Insight Manager' ('TCIM') aux failles Oracle discutées dans le bulletin d'avril 2007. IBM recommande la mise à jour du moteur "RDBMS" de 'TCIM' avant l'application des correctifs Oracle.

http://www-1.ibm.com/support/docview.wss?uid=swg21268889

Déni de service dans 'IBM HTTP Server'

Une alerte Sécunia nous informe d'une faille dans le produit 'IBM HTTP Server' qui permet à un attaquant de générer un déni de service. Cette vulnérabilité correspond à celle discutée dans un précédent bulletin sur le module Apache 'mod_proxy'.

http://secunia.com/advisories/26722

CVE-2007-3847

KDE

Publication du document advisory-20070914-1

Le projet KDE a publié le document advisory-20070914-1 concernant de nouveaux correctifs pour le navigateur 'Konqueror' corrigeant les failles CVE-2007-4224, CVE-2007-4225 et CVE-2007-3820. Ces failles permettent à un attaquant distant de mener des attaques de type "Phishing".

http://www.kde.org/info/security/advisory-20070914-1.txt

CVE-2007-3820, CVE-2007-4224, CVE-2007-4225

LINUX DEBIAN

Disponibilité de nombreux correctifs

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

linux-2.6	*DSA-1363*	*vim*	*DSA-1364*	*id3lib3.8.3*	*DSA-1365*
clamav	*DSA-1366*	*krb5*	*DSA-1367*	*librpcsecgss*	*DSA-1368*
gforce	*DSA-1369*	*phpmyadmin*	*DSA-1370*	*phpwiki*	*DSA-1371*
xorg-server	*DSA-1372*	*ktorrent*	*DSA-1373*	*jffnms*	*DSA-1374*
openoffice	*DSA-1375*	*kdebase*	*DSA-1376*	*fetchmail*	*DSA-1377*

http://www.debian.org/security/2007/

LINUX FEDORA

Disponibilité de nombreux correctifs

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

fetchmail	*Core6*	*FEDORA-2007:689*	*Fedora7*	*FEDORA-2007:1983*
krb5	*Core6*	*FEDORA-2007:690*	*Fedora7*	*FEDORA-2007:2017*
kernel2.6	*Core6*	*FEDORA-2007:679*		
claws-mail			*Fedora7*	*FEDORA-2007:2009*
wavoom			*Fedora7*	*FEDORA-2007:1977*
mapserver			*Fedora7*	*FEDORA-2007:2018*
gallery			*Fedora7*	*FEDORA-2007:2020*
clamav			*Fedora7*	*FEDORA-2007:2050*
gd	*Core6*	*FEDORA-2007:692*	*Fedora7*	*FEDORA-2007:2055*
snort			*Fedora7*	*FEDORA-2007:2060*
krb5	*Core6*	*FEDORA-2007:694*	*Fedora7*	*FEDORA-2007:2066*
qgit			*Fedora7*	*FEDORA-2007:2108*
lighttpd			*Fedora7*	*FEDORA-2007:2132*
wordpress			*Fedora7*	*FEDORA-2007:2143*
samba			*Fedora7*	*FEDORA-2007:2145*
mediawiki			*Fedora7*	*FEDORA-2007:2189*
quagga			*Fedora7*	*FEDORA-2007:2196*

cacti			Fedora7	FEDORA-2007:2199
openoffice				
qt	Core6	FEDORA-2007:700		
elinks			Fedora7	FEDORA-2007:2224
libsndfile			Fedora7	FEDORA-2007:2236
httpd	Core6	FEDORA-2007:707		
php	Core6	FEDORA-2007:709	Fedora7	FEDORA-2007:2215
kernel	Core6	FEDORA-2007:712	Fedora7	FEDORA-2007:2298
fuse			Fedora7	FEDORA-2007:2295
ntfs			Fedora7	FEDORA-2007:2295
bugzilla			Fedora7	FEDORA-2007:2299

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 :

Clamav	MDKSA-2007 172	2007	2007.1	CS3.0	CS4.0	
tar	MDKSA-2007 173	2007	2007.1		CS4.0	
krb5	MDKSA-2007 174	2007	2007.1		CS4.0	
eggdrop	MDKSA-2007 175	2007	2007.1	CS3.0		
konqueror	MDKSA-2007 176	2007	2007.1	CS3.0	CS4.0	
MySQL	MDKSA-2007 177	2007	2007.1		CS4.0	
x11-server	MDKSA-2007 178	2007	2007.1			
fetchmail	MDKSA-2007 179	2007	2007.1	CS3.0	CS4.0	
id3lib	MDKSA-2007 180	2007	2007.1	CS3.0		
librpcsecgss	MDKSA-2007 181	2007	2007.1		CS4.0	
quagga	MDKSA-2007 182				CS4.0	
qt	MDKSA-2007 183	2007	2007.1	CS3.0	CS4.0	
cacti	MDKSA-2007 184				CS4.0	
avahi	MDKSA-2007 185	2007	2007.1			
openoffice	MDKSA-2007 186	2007	2007.1	CS3.0		
php	MDKSA-2007 187	2007	2007.1	CS3.0	CS4.0	MNF2.0
postgresql	MDKSA-2007 188	2007	2007.1	CS3.0	CS4.0	

http://www.mandriva.com/security

LINUX REDHAT

Disponibilité de nombreux correctifs

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

Mysql	RHSA-2007:0875-01			AS.ES.WS 4.0	AS.ES.WS 5.0
cyrus-sasl	RHSA-2007:0795-01			AS.ES.WS 4.0	
kernel	RHSA-2007:0774-01			AS.ES.WS 4.0	
aide	RHSA-2007:0539-01				AS.ES.WS 5.0
krb5	RHSA-2007:0858-01				AS.ES.WS 5.0
cyrus-sasl	RHSA-2007:0878-01		AS.ES.WS 3.0		
star	RHSA-2007:0873-01		AS.ES.WS 3.0	AS.ES.WS 4.0	
krb5	RHSA-2007:0892-01				AS.ES.WS 5.0
mysql	RHSA-2007:0894-01			AS.ES.WS 4.0	
kernel	RHSA-2007:0705-01				AS.ES.WS 5.0
qt	RHSA-2007:0883-01	AS.ES.WS 2.1	AS.ES.WS 3.0	AS.ES.WS 4.0	AS.ES.WS 5.0
openoffice	RHSA-2007:0848-01		AS.ES.WS 3.0	AS.ES.WS 4.0	AS.ES.WS 5.0
xorg	RHSA-2007:0898-01			AS.ES.WS 4.0	
libvorbis	RHSA-2007:0845-01		AS.ES.WS 3.0	AS.ES.WS 4.0	AS.ES.WS 5.0
nfsutils	RHSA-2007:0913-01			AS.ES.WS 4.0	
php	RHSA-2007:0890-01			AS.ES.WS 4.0	AS.ES.WS 5.0
gimp	RHSA-2007:0513-01	AS.ES.WS 2.1	AS.ES.WS 3.0	AS.ES.WS 4.0	AS.ES.WS 5.0
php	RHSA-2007:0889-01		AS.ES.WS 3.0	AS.ES.WS 4.0	AS.ES.WS 5.0
tomcat	RHSA-2007:0871-01				AS.ES.WS 5.0

http://www.linuxsecurity.com/content/blogcategory/98/110/

LINUX SuSE

Disponibilité de nombreux correctifs

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

opera 9.23	SUSE-SA:2007:050
kernel	SUSE-SA:2007:051
openoffice	SUSE-SA:2007:052
Summary Report 18	SR_2007_18

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

MIT

Nouveau correctif pour la faille CVE-2007-3999

Un message publié sur la liste de diffusion Bugtraq nous annonce que le correctif pour la faille référencée CVE-2007-3999 introduit un débordement de buffer sous certaines conditions. Un nouveau correctif est maintenant disponible.

http://marc.info/?l=bugtraq&m=118902701009290&w=2

CVE-2007-3999

NETBSD

Correctifs 'IPv6' pour 'NetBSD'

Le projet NetBSD a annoncé, dans le bulletin NetBSD-SA2007-005, la disponibilité de correctifs pour 'IPv6' sur 'NetBSD' versions 2.0 à 4.0 Beta2. Ils corrigent la faille référencée CVE-2007-2242 dans le traitement des en-têtes de routage 'Type 0' du protocole 'IPv6'. Elle permet à un attaquant distant de provoquer un déni de service.

http://archives.neohapsis.com/archives/netbsd/2007-q3/0032.html

CVE-2007-2242

Correctifs pour 'BIND'

Le projet NetBSD a annoncé, dans le bulletin NetBSD-SA2007-007, la vulnérabilité de 'NetBSD' versions 2.0 à 4.0 Beta2 aux failles 'BIND' référencées CVE-2007-2926 et CVE-2007-2930. Elles permettent de provoquer la corruption du cache d'un serveur 'DNS' vulnérable. Des correctifs sont disponibles.

http://archives.neohapsis.com/archives/netbsd/2007-q3/0036.html

CVE-2007-2926, CVE-2007-2930

ORACLE

Complément d'information sur les failles 'JInitiator'

Un message publié sur la liste de diffusion Full-Disclosure apporte des informations complémentaires concernant les débordements de pile récemment discutées dans le contrôle ActiveX 'beans.ocx' du produit Oracle 'JInitiator'. Ils affectent les versions 1.1.8.3 à 1.1.8.25 de 'JInitiator', et la référence CVE CVE-2007-4467 a été attribué à ces failles.

http://lists.grok.org.uk/pipermail/full-disclosure/2007-September/065735.html

CVE-2007-4467

PANDA

Correctifs pour 'Panda Antivirus' version 2008

Panda a annoncé la disponibilité d'un correctif pour 'Panda Antivirus' version 2008. Il corrige des droits trop laxistes sur des fichiers disponibles dans le répertoire d'installation du produit qui autorisent un utilisateur local malveillant à remplacer un exécutable par un code malicieux qui sera exécuté au prochain redémarrage du système (élévation de privilèges).

http://www.pandasecurity.com/homeusers/support/card?id=41111&idIdioma=2&ref=PAV08Dev

SGI

Correctif cumulatif #80 pour SGI ProPack 3 SP6

SGI a annoncé, dans le bulletin 20070901-01-P, la disponibilité du correctif cumulatif "Security Update #80" (correctif 10448) pour SGI ProPack 3 SP6 sur plate-forme Altix. Ils corrigent des failles dans les produits 'cyrus-sasl', 'qt' et 'star'.

ftp://patches.sgi.com/support/free/security/advisories/20070901-01-P.asc

CVE-2006-1721, CVE-2007-0242, CVE-2007-4134, CVE-2007-4137

SUN

Faille 'BIND' (CVE-2007-2930) dans 'Solaris'

Sun a annoncé, dans le bulletin 103063, la vulnérabilité du serveur DNS 'BIND' version 8, fourni avec Sun 'Solaris', à la faille référencée CVE-2007-2930. Elle permet à un attaquant de corrompre le cache d'un serveur vulnérable. Sun a publié des correctifs temporaires pour les versions 8 et 9 de 'Solaris'.

http://sunsolve.sun.com/search/document.do?assetkey=1-26-103063-1

CVE-2007-2930

Faille CVE-2007-2834 dans StarOffice et StarSuite

Sun a annoncé, dans le bulletin 102994, la vulnérabilité des produits 'StarOffice' et 'StarSuite' versions 6, 7 et 8 à la faille 'OpenOffice' référencée CVE-2007-2834. Cette faille, de multiples débordements de buffer dans le code gérant les images 'TIFF', permet d'exécuter du code arbitraire. Sun fournit des correctifs pour les produits listés.

http://sunsolve.sun.com/search/document.do?assetkey=1-26-102994-1

CVE-2007-2834

Publication du document 103060

Sun a annoncé dans le document 103060 la vulnérabilité du démon 'Kerberos Administration' fourni dans les produits 'Solaris versions 8, 9, et 10 aux failles référencées CVE-2007-3999 et CVE-2007-4000. Des correctifs temporaires sont disponibles.

http://sunsolve.sun.com/search/document.do?assetkey=1-26-103060-1&searchclause=

http://www.sunsolve.sun.com/tpatches.

CVE-2007-3999, CVE-2007-4000

Révision du bulletin 102866

Sun a révisé le bulletin 102866 concernant une faille dans l'implémentation du protocole 'IP' dans 'Solaris' qui autorise un attaquant distant à provoquer un déni de service d'une plate-forme vulnérable. Cette révision annonce la mise à jour des sections "Contributing Factors" et "Resolution".

http://sunsolve.sun.com/search/document.do?assetkey=1-26-102866-1

Révision du bulletin 102866

Sun a révisé le bulletin 102866 concernant une faille dans l'implémentation du protocole 'IP' dans 'Solaris' qui autorise un attaquant distant à provoquer un déni de service d'une plate-forme vulnérable. 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=1-26-102866-1

Révision du bulletin 102874

Sun a révisé le bulletin 102874 concernant une vulnérabilité dans 'Sun Cluster' qui permet à un utilisateur local de provoquer un déni de service d'une machine vulnérable. 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=1-26-102874-1

Révision du bulletin 102927

Sun a révisé le bulletin 102927 concernant de multiples débordement de buffer dans le module 'SOCKS' de 'Sun Java System Web Proxy Server' qui peuvent permettre à un attaquant distant d'exécuter du code arbitraire. Cette révision annonce la mise à jour des sections "Contributing Factors" et "Resolution".

http://sunsolve.sun.com/search/document.do?assetkey=1-26-102927-1

Révision du bulletin 102927

Sun a révisé le bulletin 102927 concernant de multiples débordements de buffer dans le module 'SOCKS' de 'Sun Java System Web Proxy Server' qui peuvent permettre à un attaquant distant d'exécuter du code arbitraire. Cette révision annonce la mise à jour des sections "Contributing Factors" et "Resolution".

http://sunsolve.sun.com/search/document.do?assetkey=1-26-102927-1

Révision du bulletin 102945

Sun a révisé le bulletin 102945 concernant la vulnérabilité des produits 'Sun Java System Application Server', 'Sun Java System Web Server' et 'Sun Java System Web Proxy Server' aux failles, référencées CVE-2007-0008 et CVE-2007-0009, affectant la bibliothèque 'NSS'. 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=1-26-102945-1

CVE-2007-0008, CVE-2007-0009

Révision du bulletin 103018

Sun a révisé le bulletin 103018 concernant la vulnérabilité du serveur DNS 'BIND' fourni avec 'Solaris' version 10 à la faille référencée CVE-2007-2926 qui permet à un attaquant de corrompre le cache DNS d'un serveur. Cette révision annonce la mise à jour de la section "Resolution".

http://sunsolve.sun.com/search/document.do?assetkey=1-26-103018-1

CVE-2007-2926

CODES D'EXPLOITATION

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

APPLE

Code d'exploitation pour la faille CVE-2007-2394

Un code d'exploitation a été publié sur le site Web Milw0rm exploitant la faille Apple référencée CVE-2007-2394. Cette vulnérabilité, un débordement d'entier déclenché par un fichier 'SMIL' spécialement construit, permet d'exécuter du code arbitraire ou de provoquer un déni de service. Ce code permet de générer un fichier 'SMIL' spécialement construit qui provoquera un déni de service du lecteur lorsqu'il sera ouvert par le lecteur vulnérable.

http://milw0rm.com/exploits/4359

CVE-2007-2394

TREND MICRO

Code d'exploitation pour la faille CVE-2007-1070

Un code d'exploitation a été publié sur le site Web Milw0rm exploitant la vulnérabilité Trend Micro référencée CVE-2007-1070, dans la bibliothèque 'eng50.dll' des produits 'ServerProtect'. Ce code permet de provoquer un débordement de pile dans un serveur vulnérable distant afin d'obtenir un interpréteur de commandes.

http://milw0rm.com/exploits/4367

CVE-2007-1070

BULLETINS ET NOTES

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

MICROSOFT

Disponibilité du Service Pack 3 pour Office 2003

Microsoft a annoncé la disponibilité du Service Pack 3 pour Office 2003. Il apporte de nombreuses améliorations et une meilleure stabilité, et inclut les correctifs de sécurité MS06-062, MS06-061, MS06-048, MS06-038, MS06-039, MS06-009, MS06-037, MS06-012, MS06-003, MS06-028, MS06-054, MS06-027, MS07-044, et MS07-042.

http://support.microsoft.com/kb/923618

http://www.microsoft.com/downloads/details.aspx?FamilyID=e25b7049-3e13-433b-b9d2-5e3c1132f206&displaylang=en#QuickInfoContainer

CVE-2005-4131, CVE-2006-0001, CVE-2006-0002, CVE-2006-0007, CVE-2006-0008, CVE-2006-0009, CVE-2006-0022, CVE-2006-0028, CVE-2006-0029, CVE-2006-0030, CVE-2006-0031, CVE-2006-0033, CVE-2006-1301, CVE-2006-1302, CVE-2006-1304, CVE-2006-1306, CVE-2006-1308, CVE-2006-1309, CVE-2006-1316, CVE-2006-1540, CVE-2006-2388, CVE-2006-2389, CVE-2006-2492, CVE-2006-3059, CVE-2006-3434, CVE-2006-3449, CVE-2006-3590, CVE-2006-3650, CVE-2006-3864, CVE-2006-3868, CVE-2006-4685, CVE-2006-4686, CVE-2007-2223, CVE-2007-3890

SYMANTEC

Publication du document SYM07-024

Symantec a publié le document SYM07-024 concernant une faille dans le pilote 'symtdi.sys' qui permet de provoquer un déni de service de certains produits Symantec. Ce document annonce la vulnérabilité des produits 'Norton AntiSpam', 'Norton AntiVirus', 'Norton Internet Security', 'Norton Personal Firewall', 'Norton System Works', 'Symantec AntiVirus Corporate Edition', 'Symantec AntiVirus Corporate Edition', 'Symantec AntiVirus Corporate Edition', et 'Symantec Client Security'. Des correctifs sont disponibles via la fonctionnalité "LiveUpdate" et Symantec met également à disposition un outil pour mettre à jour le pilote.

http://service1.symantec.com/SUPPORT/ent-security.nsf/docid/2007090409431648

http://www.symantec.com/avcenter/security/Content/2007.09.05.html

CVE-2007-1476

VMWARE

Nouvelles versions des produits VMware

VMware a publié sur la liste de diffusion Full-Disclosure son alerte VMSA-2007-0006 concernant la disponibilité de correctifs pour les produits 'VMware ESX', 'VMware ACE', 'VMware Server', 'VMware Player', et 'VMware Workstation'. Ils corrigent de nombreuses failles qui permettent de provoquer, entre autres choses, des dénis de service et l'exécution de code arbitraire.

http://lists.grok.org.uk/pipermail/full-disclosure/2007-September/065902.html

CVE-2004-0813, CVE-2006-1174, CVE-2006-3619, CVE-2006-4146, CVE-2006-4600, CVE-2007-0061, CVE-2007-0062, CVE-2007-0063, CVE-2007-0494, CVE-2007-1716, CVE-2007-1856, CVE-2007-2442, CVE-2007-2443, CVE-2007-2446, CVE-2007-2447, CVE-2007-2798, CVE-2007-4059, CVE-2007-4155, CVE-2007-4496, CVE-2007-4497