APOGEE Communications

Rapport de Veille Technologique Sécurité N°105

Avril 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
15, Avenue du Cap Horn
ZA de Courtaboeuf
91940 Les ULIS

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 …

L'actualité du mois tourne, est-ce étonnant, autour des élections présidentielles et en particulier de l'usage des machines à voter électroniques. Les problèmes pratiques rencontrés, autant que les études de sécurité engagées dans différents pays, conduisent à se poser la question de leur réelle utilité et plus encore du niveau de confiance que l'on pourra accorder à la fiabilité des résultats produits.

Ce sujet fait l'objet d'un long mais très intéressant fil de discussion sur le groupe 'fr.misc.cryptologie' duquel il ressort que, bien qu'un profil de protection ad hoc ait été certifié en 2006, celui vise un niveau d'assurance **EAL2+** ni obligatoire ni appliqué et ridiculement faible au regard des enjeux.

Même s'il peut apparaître inefficace au regard du potentiel offert par les technologies modernes, le mode de dépouillement classique dit 'manuel' reste, et restera longtemps, l'approche la plus adaptée et, de notre point de vue, la plus citoyenne.

http://www.ssi.gouv.fr/fr/confiance/pp/pp_2006_04.html

Nous mentionnions dans notre rapport précédent, la consultation engagée par l'**AFNIC** au sujet de l'évolution du service '**Whois**'. Les résultats de cette consultation sont désormais disponibles sur le site de l'**AFNIC**. Il en ressort que la proposition de la mise en place de deux niveaux de service – un service gratuit tous publics et un service dédié aux bureaux d'enregistrement - reçoit le soutien de la majorité des contributeurs. L'ouverture d'un troisième service proposant des fonctionnalités avancées – veille, surveillance, prospection – est sujet à controverses.

http://www.afnic.fr/actu/nouvelles/general/NN20070424

Depuis maintenant près de quatre ans, nos bulletins d'alertes de sécurité intègrent systématiquement l'identifiant **CVE** correspondant aux vulnérabilités traitées lorsque celui-ci existe. Nous n'avions pour autant jamais considéré qu'il soit opportun d'obtenir le label '**service compatible CVE**' délivré par le **MITRE**, priorité étant donnée à la qualité du service plus qu'à son image de marque.

Il apparaît désormais que, notamment sur les marchés extérieurs à l'hexagone, ce référencement purement 'formel' soit un plus. Nous avons dons sauté le pas et avons le plaisir d'annoncer à nos lecteurs qu'une déclaration de compatibilité **CVE** a été transmise ce mois-ci au **MITRE**.

http://www.cve.mitre.org/news/index.html#20070406c

Bertrand VELLE

PRODUITS ET TECHNOLOGIES

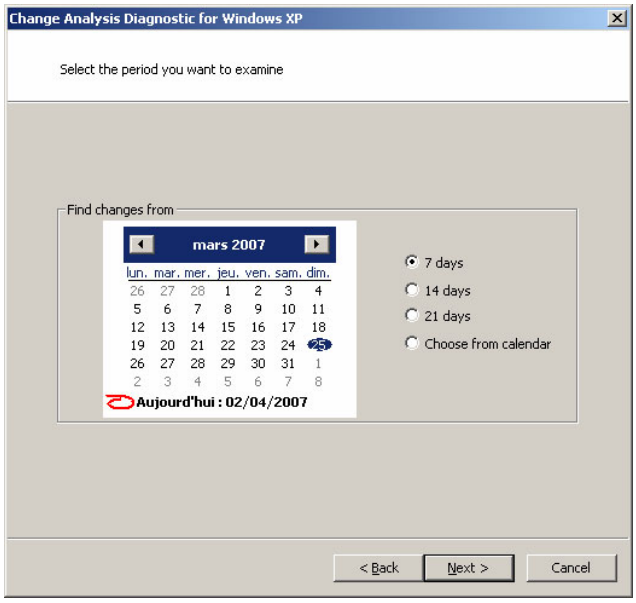
LES PRODUITS

INTEGRITE

MICROSOFT – OUTIL D'ANALYSE DES CHANGEMENTS

- **Description**

Microsoft propose au téléchargement un utilitaire dénommé '**Change Analysis Diagnostic**' permettant de visualiser les données journalisées par le système de restauration automatique du système d'exploitation **Windows XP**.



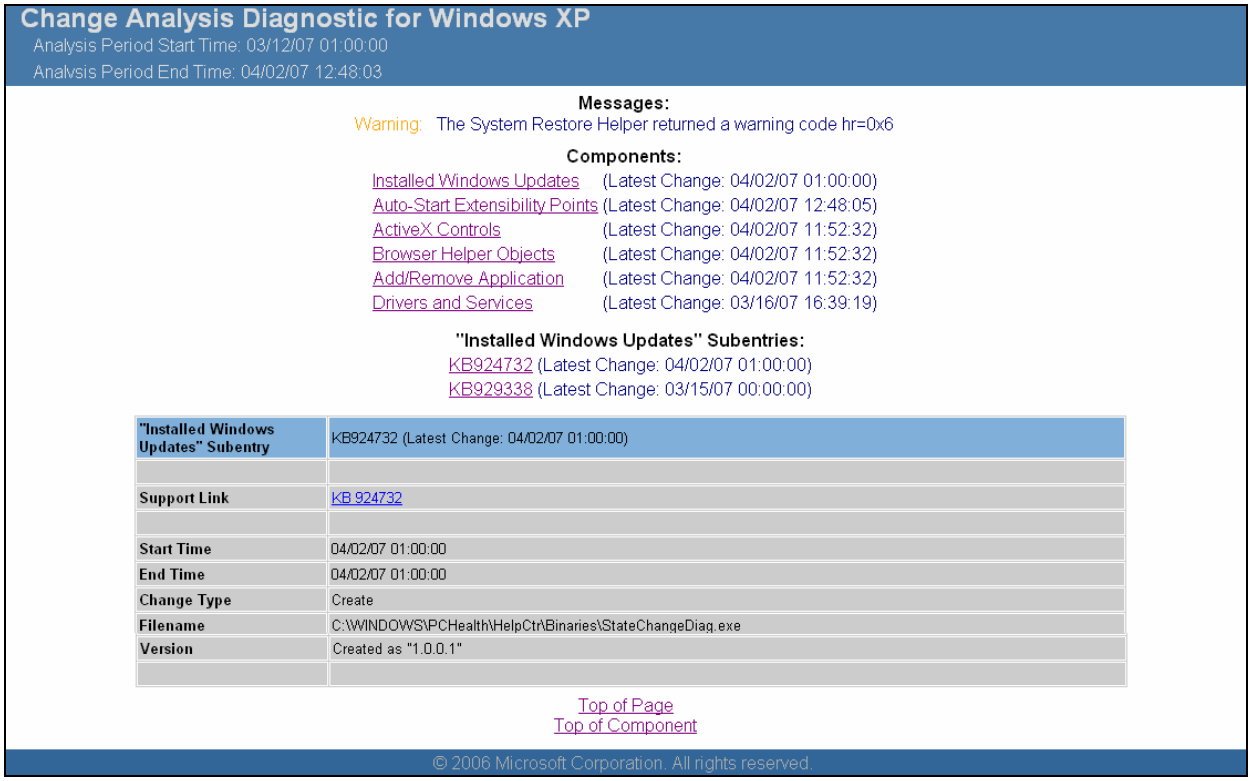
Cet utilitaire a surtout été conçu pour faciliter le travail des services de support et de maintenance, un fichier **XML** contenant toutes les modifications effectuées sur le système pouvant être généré et facilement transmis en cas de problème constaté par l'utilisateur sur son poste.

Ne pourront cependant être détectées que les seules modifications supervisées par le système de restauration sous réserve que celui-ci soit actif et que des points de restauration aient été générés.

Les modifications 'sauvages' d'un composant ou d'une application, c'est à dire effectuées par simple recopie ou destruction des ressources sans passer par les interfaces ad hoc, ne seront ainsi jamais inventoriées.

L'installation de l'outil ne pose aucune réelle difficulté à condition que la licence du système ait été correctement validée. La version actuelle ne fonctionne toutefois qu'avec un système **Windows XP** de langue Anglo-Saxonne. Ceci devrait être rapidement corrigé.

On notera par ailleurs que la procédure d'installation ne créée ni raccourci ni entrée dans la liste des programmes. L'outil devra donc être activé par le biais du menu '**Start**' via la commande '**statechangediag**'.



Il serait aussi possible de l'activer en arrière plan par le biais d'une ligne de commande afin de collecter les informations relatives aux modifications de manière totalement automatisée mais nous n'avons trouvé aucune information concernant les options permettant d'activer ce mode de fonctionnement. De même, ni l'emplacement ni le nom du fichier contenant le rapport au format '**XML**' ne semblent pouvoir être configurés.

Le dossier de présentation de l'outil annonce que celui-ci détectera certaines formes de modification portant sur:
- les applications listées par l'outil 'Ajout/Suppression de programmes',
- les composants du système dont les correctifs et mises à jour effectuées via le service Windows Update,
- les modules d'extensions chargés dans le navigateur Internet Explorer,
- les gestionnaires de périphériques,
- les contrôles Active/X enregistrés,
- les ressources activées automatiquement lors de l'ouverture d'une session.

Notre avis reste très réservé quant à la réelle utilité de cet outil dans une structure de support, outil qui n'est aucunement – comme le précise Microsoft – un outil de sécurité. Nombreux sont en effet les dysfonctionnements qui proviennent de manipulations, volontaires ou non, effectuées dans des conditions conduisant à ne pas les journaliser. Bien d'autres utilitaires sont disponibles qui permettent de tracer efficacement toutes les modifications apportées sur les ressources du système sans pré-requis d'aucune sorte.

- **Complément d'information**

http://support.microsoft.com/?kbid=924732
http://isc.sans.org/diary.html?storyid=2525

LES TECHNOLOGIES

WIFI

ARCEP – NIVEAU DES CHAMPS ELECTROMAGNETIQUES WIFI

- **Description**

L'autorité de régulation – ex **ART** - vient de rendre publics les résultats d'une étude menée pour elle par le département EMG de **Supelec** sur les niveaux des champs électromagnétiques produits par les réseaux radioélectriques (RLAN) fonctionnant dans la bande des 2.4GHz

Le terme **RLAN** est ici employé conformément à la réglementation (Décret n° 2002-775) définissant les valeurs limites d'exposition du public aux champs électromagnétiques sans limitation sur la technologie employée bien que la gamme de fréquences ici étudiée soit principalement occupée par des réseaux informatiques de type Wifi. L'étude porte cependant exclusivement sur les équipements conformes aux standards IEEE-802.11b et IEEE-802.11g.

Engagée en 2003, cette étude était constituée de deux phases complémentaires dont les résultats n'avaient jusqu'à maintenant pas été rendus publics:

- La phase I, initiée en 2003, visait à mesurer les respects des valeurs limites du débit d'absorption spécifique - ou '**DAS**' - à une distance supérieure à la longueur d'onde d'émission soit ici 12,5cm. Ce cas de figure correspond notamment à la mise en œuvre de dispositifs **Wifi** de type Point d'Accès.
- La phase II, menée en 2005, avait pour objet d'étendre ces mesures à des distances inférieures afin de traiter le cas des dispositifs embarqués dans des équipements portables utilisés au plus près de l'usager: PC portable posé sur les genoux, téléphone **Wifi**, …

Face à l'utilisation croissante de tels dispositifs et probablement pour parer aux questions que les usagers ne manqueront pas de se poser sur l'impact sanitaire de leur utilisation – rappelons que les équipements **GSM** / **DECT**, objets de nombreuses études, travaillent dans des gammes de fréquences inférieures 900Mhz et 1800/1900Mhz – l'**ARCEP** a pris le parti de publier le rapport final d'étude de la phase I (daté de décembre 2003) et la synthèse générale (datée de décembre 2006) tous deux rédigés par **Supelec**.

Cette synthèse conclut que:

> *« pour des conditions d'utilisation conformes à la réglementation radioélectrique des RLAN, les valeurs limites d'exposition du public aux champs électromagnétiques définies dans le décret n° 2002-775 sont respectées pour tous les cas d'utilisation de matériels RLAN mesurés ou simulés dans le cadre de l'étude.»*

On notera qu'il s'agit bien ici d'une validation de la conformité des équipements mesurés à la norme sans considération aucune sur l'impact ou sur les risques en cas d'exposition prolongée, cas de figure couramment rencontré dans le cas des équipements de type 'PC portable' pour lesquels la liaison radio est maintenue active à pleine puissance sur une plus grande période de temps qu'un téléphone portable.

Le document de synthèse comporte toutefois une annexe listant quelques principes élémentaires permettant de réduire notablement l'exposition, et ceci bien qu'il y soit aussi rappelé que « *bien qu'il n'y ait aucun risque avéré lié à une exposition aux champs électromagnétiques conforme aux dispositions du décret n° 2002-775, ces informations permettront aux personnes qui le désirent de limiter toute exposition inutile tout en permettant une utilisation optimale des applications de RLAN.*»

Le principe de précaution prévaut dans un domaine où l'incertitude règne et où les anciens aiment bien à rappeler des histoires d'oiseaux perdant le nord lorsqu'ils passaient dans des faisceaux radars – d'une puissance crête infiniment supérieure à celle développée par les équipements RLAN, fort heureusement – ou à citer le cas d'opérateurs n'ayant plus eu que des filles après avoir travaillé dans le champ de ces mêmes radars ou de faisceaux hertziens.

Cette étude a le grand mérite de quantifier précisément les niveaux des champs électromagnétiques émis par des équipements encore couramment utilisés en 2007 et dans des conditions d'environnement et de configuration parfaitement connues. Les données ainsi collectées pourront servir de référentiels dans le cas des nouvelles campagnes de mesures qui ne marqueront pas d'être engagées sur des technologies plus récentes. Le rapport final d'étude de la phase II n'est, à ce jour, pas disponible.

- **Complément d'information**

http://www.art-telecom.fr/index.php?id=8571&tx_gsactualite_pi1[uid]=936&cHash=ea7829e25c - Communiqué de presse
http://www.art-telecom.fr/uploads/tx_gspublication/synth-etudesupelec-wifi-dec06.pdf - Rapport final phase I
http://www.legifrance.gouv.fr/WAspad/UnTexteDeJorf?numjo=INDI0220135D - Décret 2002-775

INFORMATIONS ET LEGISLATION

LES INFORMATIONS

CONFERENCES

BLACKHAT2007 - EUROPE

- **Description**

L'édition européenne de la conférence **BlackHat** s'est tenue du 27 au 30 mars dernier à **Amsterdam**. Au total, ce sont 23 présentations qui auront été données dont une partie des supports est désormais disponible.

Nous commenterons les présentations les plus innovantes à partir des supports disponibles en proposant tout d'abord une liste des présentations, celles-ci étant classées par ordre alphabétique:

360° Anomaly Based Unsupervised Intrusion Detection	Stefano Zanero	*BH DC 07*
Advanced Oracle Attack Techniques	David Litchfield	*BH DC 07*
Attacking the Giants: Exploiting SAP Internals	Mariano Di Croce	
Challenging Malicious Inputs with Fault Tolerance Techniques	Bruno Luiz	
Countering The Faults of Typical Web Scanners	Toshinari Kureha & all	
GS and ASLR in Windows Vista	Ollie Whitehouse	*BH DC 07*
Hacking Databases for Owning Your Data	Cesar Cerrudo & all	
Heap Feng Shui in JavaScript	Alexander Sotirov	
Kernel Wars	Joel Eriksson	
Kicking Down the Cross Domain Door (One XSS at a Time)	Billy K Rios & all	
Making Windows Exploits More Reliable	Kostya Kortchinsky	
NACATTACK	Michael Thumann & all	
New Botnets Trends and Threats	Paes de Barros & all	
Next Generation Debuggers for Reverse Engineering	ERESI Team	
NIDS: False Positive Reduction Through Anomaly Detection	Damiano Bolzoni	
RFIDIOts!!! - Practical RFID hacking (without soldering irons)	Adam Laurie	
ScarabMon - Automating Web Application Penetration Tests	Jonathan Wilkins	
SCTPscan - Finding Entry Points to SS7 Networks	Philippe Langlois	
SMTP Information Gathering	Lluis Mora	
Software Virtualization Based Rootkits	Sun Bing	
Vboot Kit: Compromising Windows Vista Security	Nitin & Vipin Kumar	
Web Service Vulnerabilities	Nish Bhalla	
Wi-Fi Advanced Fuzzing	Laurent Butti	*SSTIC07*

SMTP Information Gathering — Lluis Mora

Lluis Mora, de la société espagnole **NeutralBit**, aborde ici un thème qui nous est cher: celui de la collecte d'informations publiquement accessibles et aisément valorisables, en l'occurrence et dans le cas présent, les données enregistrées dans les en-têtes de courriers électroniques au fur et à mesure de leur transit à travers les multiples systèmes de transfert dits '**MTA**'.

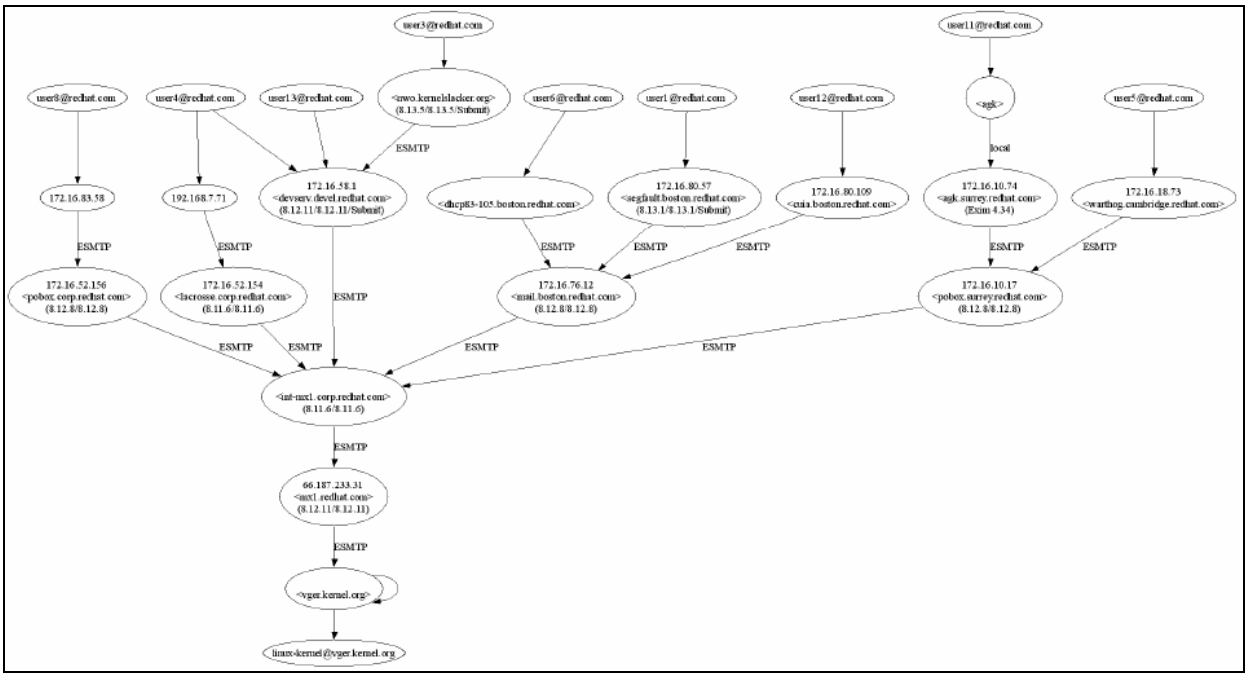
Cette présentation ne révèle rien qui ne soit déjà su ou connu mais elle a le mérite d'exposer le problème dans une forme accessible à tous et d'appuyer le message sur le risque d'utilisation détournée de ces données à l'aide de différents exemples extrêmement parlants.

Ainsi, après avoir rappelé le principe sous-jacent à la construction de ces en-têtes que l'on retrouvera dans chacun des messages échangés dans un système de messagerie conforme au standard **RFC822** et donc aussi dans les archives des listes de discussions utilisant ce support, l'auteur aborde le problème de la divulgation directe ou indirecte des informations contenues dans celles-ci.

Le cas présenté , désormais classique, est celui de la reconstitution d'une partie du plan d'adressage, si ce n'est de la structure du réseau interne d'une société, par le biais des adresses et noms des serveurs ayant servis à relayer le message du client jusqu'au point d'accès Internet.

L'agrégation de ces informations permet de disposer d'une vue de plus en plus détaillée de l'architecture en inventoriant chacun des serveurs internes et en offrant la possibilité de reconstituer, brique par brique, la topologie en usage: noms et adresses des systèmes mais aussi localisation géographique partielle par l'indication du fuseau horaire de chacun d'entre eux.

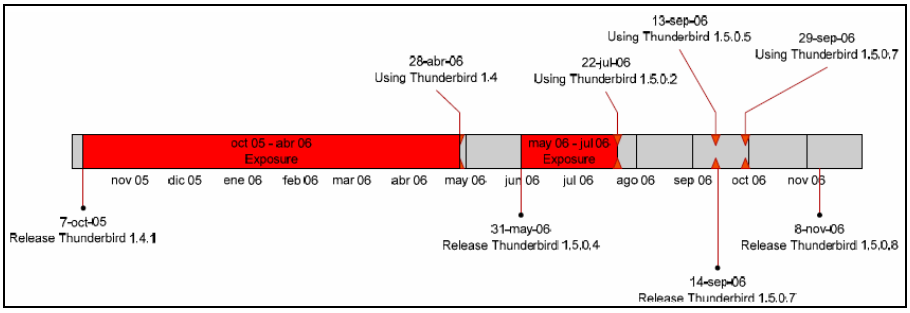
Bien que l'analyse des structures des en-têtes ne soit pas une tâche aussi triviale qu'il pourrait y paraître au premier abord, l'auteur s'est penché sur un exercice fort instructif: l'analyse des en-têtes des courriers échangés sur une liste de diffusion pour une période de 3 mois au début de l'année 2006. Il lui a ainsi été possible de reconstruire les topologies des systèmes de messagerie de plusieurs sociétés dont **SuSE** et **RedHat**.



L'exemple présenté ci-dessus – routage des mails dans le domaine '**redhat.com**' – pour anodin qu'il puisse paraître pourrait permettre à un éventuel agresseur d'améliorer l'efficacité d'un code malicieux astucieusement injecté dans l'infrastructure interne pour être exécuté sur un poste client. Et ce n'est ici qu'une exploitation parmi d'autres des données ainsi patiemment agrégées.

L'auteur s'intéresse ensuite à l'exploitation des informations ayant été positionnées dans l'en-tête, non pas par les serveurs relais mais par le client à l'origine du message. Ici encore, une campagne d'analyse et de corrélation de ces données peut s'avérer extrêmement riche d'enseignement pour quiconque dispose du temps nécessaire.

L'auteur a ainsi pu établir, a posteriori mais sans autres données que celles présentes dans les messages transmis par un tiers, l'échéancier des mises à jour du client de messagerie utilisé par ce tiers! De là à en déduire la politique de mise à jour en vigueur dans l'entreprise il n'y qu'un pas qu'il est aisé de franchir.



Bien d'autres informations peuvent être déduites des divers champs présents dans les en-têtes: politique de filtrage des spams, de protection contre les virus, …

http://www.neutralbit.com/en/rd/articles/ - Complément d'information

Challenging Malicious Inputs with Fault Tolerance Techniques — Bruno Luiz

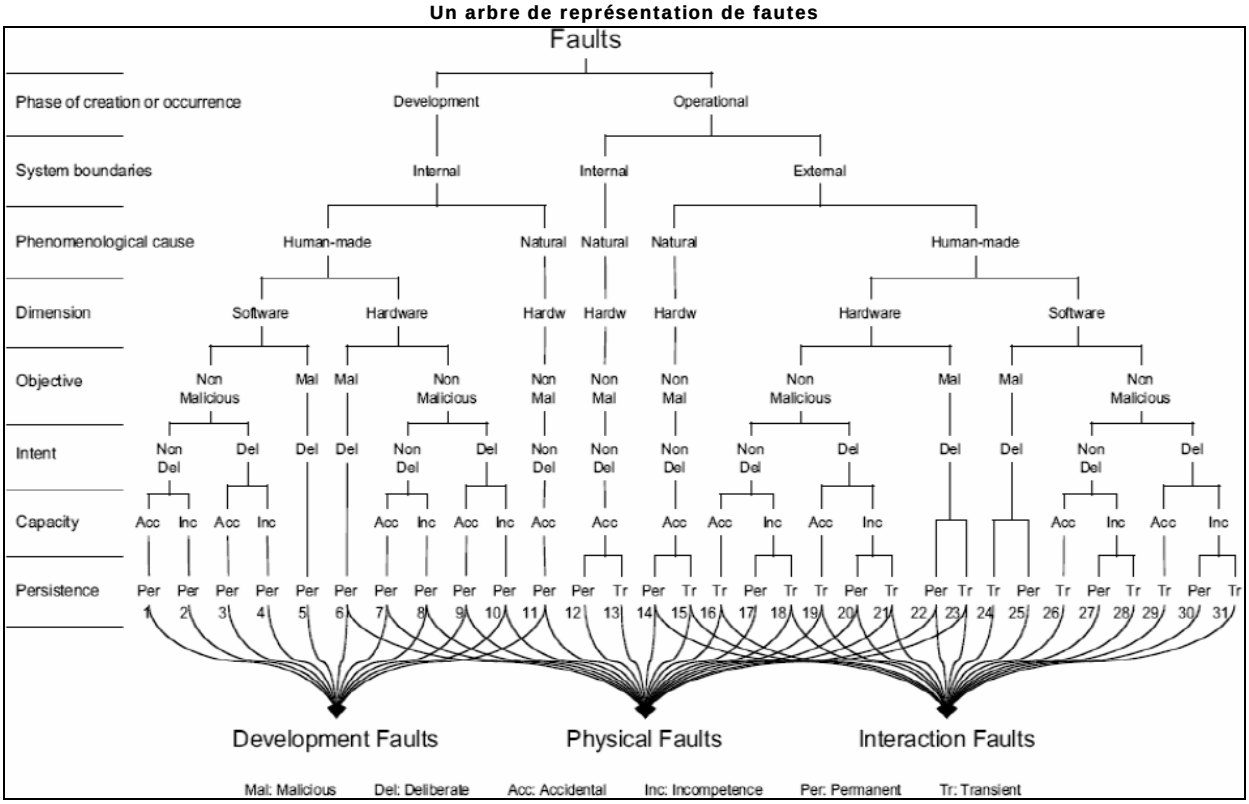
Bruno Luiz, un étudiant et chercheur de l'université catholique du **Brésil**, tente de démontrer que l'utilisation de techniques issues de la conception de systèmes tolérants aux pannes peut faciliter la détection de la manipulation des données d'entrée d'un programme voire même protéger une application pourtant vulnérable contre l'injection de fautes arbitraires, une technique connue sous le nom de '**Fuzzing**'.

Il est vrai que nombreux sont les parallèles pouvant être mis en évidence entre les domaines de la sûreté de fonctionnement d'un système et de la sécurité de ce même système. Les deux approches ont au moins en commun un objectif majeur: garantir que le comportement du système ne dévie pas de celui pour lequel il a été spécifié.

Si les principes fondamentaux de la sûreté de fonctionnement visent à minimiser l'impact d'une quelconque faute à l'aide de procédés généralement regroupés sous le terme de 'tolérance aux pannes', ceux de la sécurité ont traditionnellement pour objectif d'éliminer tout risque d'atteinte au bon fonctionnement du système, objectif que l'on tente d'atteindre en réduisant l'exposition de ce dernier aux bogues de conception et de réalisation. En partant du principe qu'un code expurgé de toute erreur ne peut exister, force est d'admettre que l'approche de la sûreté de fonctionnement ne peut qu'amener à améliorer la sécurité du système.

Dans son exposé, l'auteur n'aborde que brièvement les principes conduisant à minimiser les erreurs au niveau de la conception pour se concentrer sur les méthodes de détection et de correction des fautes: redondance des données, duplication des calculs, vérification de la consistance, récupération avant ou arrière, … autant de techniques permettant d'identifier l'existence d'un problème et de le corriger avant qu'il ne puisse impacter l'intégrité de la fonction ou du service et qui pourront être mises en œuvre pour compenser les vulnérabilités résiduelles d'une application.

Un arbre de représentation de fautes



Les langages modernes autorisent une mise en œuvre assez aisée de ces différentes techniques par le biais de mécanismes de validation et de gestion des exceptions plus ou moins évolués, les processeurs actuels offrant la possibilité d'implémenter des mécanismes d'exécution simultanée et de vote majoritaire avec un impact réduit sur les performances globales du système.

L'auteur conclut son propos par la présentation d'une stratégie de gestion des traitements des données d'entrée d'une application permettant de masquer les dysfonctionnements qui ne manqueraient pas d'être normalement révélés par l'utilisation d'un outil d'injection de fautes.

http://www.cs.cornell.edu/Projects/secft/ - Une tentative d'intégration des deux approches

Attacking the Giants: Exploiting SAP Internals — Mariano Di Croce

Avec cette présentation qui s'attaque à la sécurité de l'un des logiciels de gestion intégrée les plus connus, **Mariano Di Croce** - qui travaille pour la société de conseil '**CybSec SA**' présente en Amérique du Sud - a fait la Une de la plupart des sites s'intéressant à la sécurité. Et il y a de quoi …

L'architecture du progiciel **SAP** y est décortiquée en mettant en évidence la remarquable conception de ce progiciel aisément extensible car organisé autour d'un bus logiciel qui utilise intensivement un mécanisme d'appel de procédures distantes ou **RPC**. Une interface de communication dénommée **SAP RFC** (SAP **R**emote **F**unction **C**all) forme le cœur de cette architecture et facilite l'interconnexion des modules applicatifs écrits aussi en langages **.NET**, **VB** ou encore en **Java** via le connecteur dédié.

Très bien documentée, efficace et offrant toutes les fonctionnalités requises pour le développement de modules de traitement spécifiques, cette interface peut cependant se révéler offrir un fabuleux terrain de jeu pour qui saurait tirer parti de ses qualités et ses défauts. Celle-ci a en effet été conçue à la fin des années 80, à une époque où il était d'usage de considérer qu'il était de la responsabilité des utilisateurs d'une interface d'accès d'utiliser celle-ci conformément aux spécifications et de ne fournir que des paramètres valides. Facteur aggravant s'il en est, les données sont, par défaut, transmises en clair et éventuellement compressées, les mots de passe faisant l'objet d'un masquage trivial, à savoir un OU exclusif avec une clef constante.

Comment alors s'étonner qu'il soit possible de collecter les mots de passe des connexions par une simple analyse des échanges ou encore de provoquer un dysfonctionnement sévère des serveurs par un appel, non conforme aux spécifications, de certaines fonctions sans oublier la possibilité de lister sans aucune contrainte d'aucune sorte les fonctions offertes par un serveur, un classique du genre.

Après avoir parcouru quelques unes des fonctions les plus intéressantes pour le plaisir et le profit de l'usager curieux, l'auteur présente quelques scénarios d'attaque dont l'enregistrement d'un serveur tiers dans une architecture existante à des fins d'interception et de détournement des requêtes.

Un outil modulaire d'analyse dénommé '**SAPYTO**' écrit en '**C**' et en '**Python**' a été développé par l'auteur afin d'automatiser l'audit des architectures **SAP R/3**. Non encore finalisé, cet outil dispose déjà de nombreux modules implémentant des fonctions de collecte d'informations mais aussi d'attaque.

Pour conclure, l'auteur rappelle que la simple activation du mécanisme de chiffrement **SNC** (Secure Network Communications) livré avec **SAP** permettrait de réduire la surface d'exposition d'une infrastructure **SAP** en rendant inopérant les mécanismes de collecte des données circulant sur le réseau.

L'application des mises à jour de sécurité 1005397, 1003908 et 1003910 résout les (premiers) problèmes de sécurité découverts dans les fonctions de l'interface **SAP RFC**.

http://cybsec.com/EN/articles/default.php - Articles complémentaires
http://www.cybsec.com/vuln/tools/sapyto.tgz - Outil d'analyse **SAPYTO**

SCTPscan - Finding Entry Points to SS7 Networks — Philippe Langlois

Assurée par **Philippe Langlois**, cette présentation porte sur le système de signalisation du réseau téléphonique classique, dit **SS7**, et aux risques induits par l'interconnexion d'un monde par définition fermé – le **RTC** – avec le monde ouvert des réseaux **IP**.

Elle commence par un rappel fort intéressant des spécificités de ce système de signalisation numérique d'origine Européenne qui dispose de son propre réseau de transport contrairement aux systèmes qui furent en vigueur dans d'autres pays dont les **USA** où la signalisation était transmise dans la bande sous la forme de séquences sonores. Contrairement donc à ces réseaux où le poste client offrait à tous un accès au système de signalisation par le biais de dispositifs appelés boîtes – ou boxes – essentiellement constituées d'un générateur de tonalités permettant l'injection de signaux de commande, l'infrastructure de signalisation **SS7** garantit une excellente protection en découplant la signalisation et le transport de la voix sans qu'aucun point d'accès, hors la numérotation, ne soit offert à l'usager lambda. S'insérer dans ce réseau supposait alors de disposer d'un accès sur les liaisons numériques utilisées par l'opérateur dans son cœur de réseau, une opération qui n'était pas à la portée de tous.

Les choses ont totalement changé avec l'avènement de la téléphonie sur IP, et le transport de cette même signalisation **SS7** à travers un réseau ouvert, l'Internet, et par le biais d'un service accessible par les mêmes moyens que tous les autres services **IP**.

Le cœur de réseau est ainsi désormais constitué d'une multitude d'équipements spécialisés interconnectés par le biais du protocole **SCTP** – une adaptation du protocole **TCP** permettant de prendre en compte les contraintes liées à la diffusion de flux à forte contrainte temporelle - lequel assure le transport de la voix et la signalisation. La gestion de cette dernière est effectuée en conformité avec une série de standards **IETF** regroupés sous la dénomination '**SIGTRAN**'.

Les cœurs de réseau des opérateurs de télécommunication utilisant ces nouvelles technologies seront généralement protégés par l'utilisation d'infrastructures de transport privatives, les services associés étant alors inaccessibles depuis l'Internet. Cette précaution est d'autant plus vitale pour le bon fonctionnement du réseau qu'il est non seulement aisé de déterminer la présence d'un service **SCTP** actif sur un système mais aussi l'existence d'un point d'entrée sur le réseau de signalisation.

Dans la seconde partie de sa présentation, **Philippe Langlois** nous dévoile différents procédés de sondage plus ou moins discrets intégrés dans un utilitaire dénommé '**SCTPScan**' permettant d'automatiser la recherche des services **SCTP**. Cette automatisation est hélas largement facilitée par la nature même des services sur l'Internet et de certaines des fonctionnalités natives du service **SCTP**. Cet utilitaire devrait évoluer pour intégrer une fonction d'identification des applications par analyse de leur empreinte ainsi qu'un mécanisme de fuzzing destiné à valider la robustesse des implémentations lors du traitement de structures protocolaires contenant des données aléatoires.

L'utilisation de l'outil d'analyse réseau '**WireShark**' – ex. **Ethereal** – et du dissecteur **SCTP** permettra ensuite de remonter dans les couches hautes du protocole – services **SUA**, **M3UA**, **TCAP**, **MAP**, **CAP**, **INAP**, … - lesquelles n'ont plus rien à voir avec le monde **IP** et sont donc peu connues en dehors des spécialistes.

Cette présentation et la mise à disposition de l'utilitaire '**SCTP**' pourraient bien donner des idées à nombre de bidouilleurs d'autant que certains documents de spécifications de l'**ITU** – dont ceux de la série **Q** – sont, comme le souligne l'auteur, désormais librement accessibles.

On notera par ailleurs qu'en juin 2004 était publié le **RFC3788** intitulé '**Security Considerations for Signaling Transport (SIGTRAN) Protocols**' qui, après avoir rappelé la relative fragilité des services de signalisation sur des réseaux non sûrs, posait comme principe de base l'utilisation d'un transport sécurisé - **IPSec** par défaut et **TLS** en option – en rappelant l'absolue nécessité de disposer d'une infrastructure de gestion des éléments de sécurité associés.

http://sctp.tstf.net/index.php/SCTPscan/SCTPscan - SCTPScan
http://www.itu.int/ITU-T/worksem/security/200510/abstracts/s7-leber.pdf - Workshop ITU 2005
http://www.itu.int/search/pages/ituwebsearch/basic.asp?QuerySubmit=true&QueryText=SS7 - Tout sur la SS7 à l'ITU

- **Complément d'information**

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

VEILLE

ENISA - LA REVUE

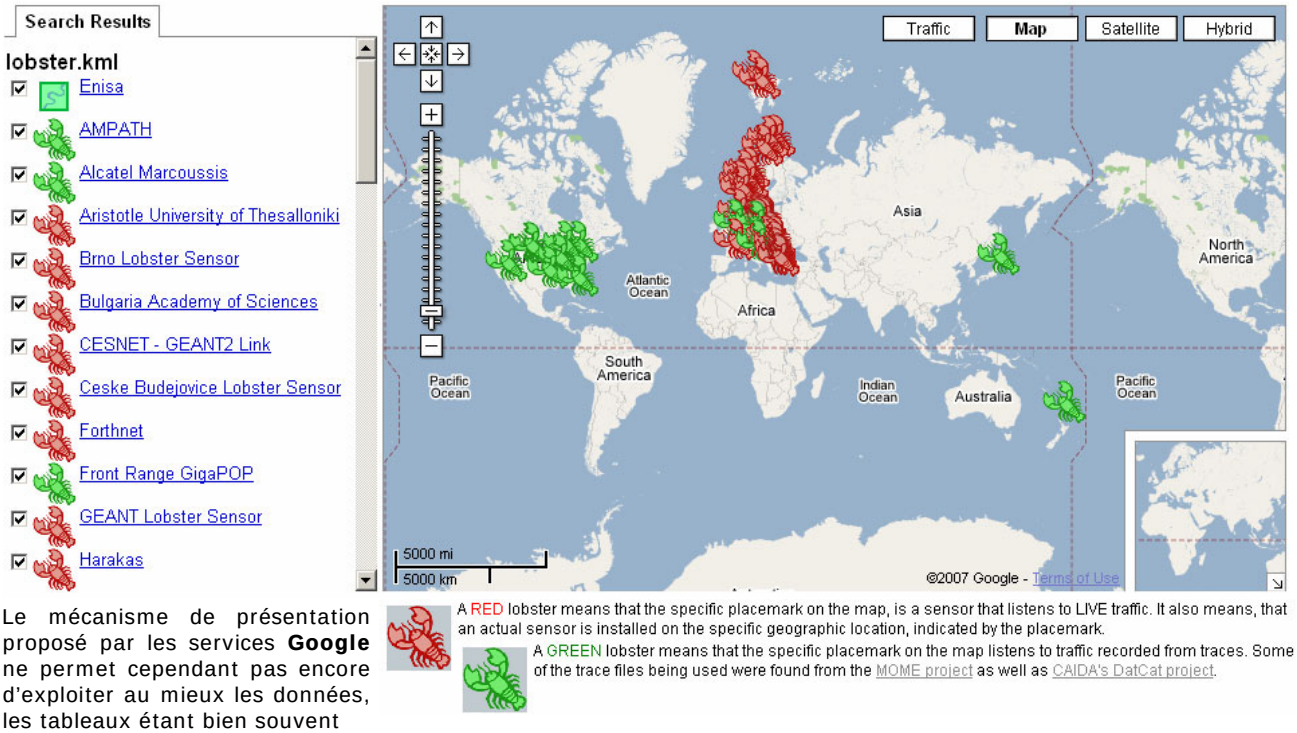
- **Description**

Un nouveau numéro de la revue '**ENISA Quarterly**' (dont la notoriété croit puisque plus de 10 000 exemplaires sont désormais téléchargés par mois) est paru. Celui-ci, qui comporte plus d'articles que les numéros précédents, est plus particulièrement consacré au thème des systèmes de détection et d'alerte avancée ou **EWS** (Early Warning System).

Après une intéressante présentation des principes mis en œuvre dans de tels systèmes (article '**Probe-based Internet Early Warning System**'), une description détaillée des infrastructures de surveillance passive '**LOBSTER**' (Large scale monitoring of broadband Internet infrastructure) etde capture de données

'**NOAH**' est proposée (article '**Real-time Monitoring and Detection of Cyberattacks**').

Déployé dans le cadre d'un projet Européen, le réseau '**LOBSTER**' est constitué d'un grand nombre de sondes purement passives réparties principalement en Europe – dont une sonde dans les laboratoires Alcatel de Marcoussis – mais aussi aux Etats-Unis et au Japon. Une cartographie en temps réel des sondes fonctionnelles, et du trafic collecté, est proposée par le biais d'un module additionnel venant se greffer sur les services Google Maps et Google Earth. Le résultat est absolument remarquable et parfaitement représentatif de ce que l'on peut obtenir par une judicieuse combinaison des services actuellement offerts par l'Internet.



Le mécanisme de présentation proposé par les services **Google** ne permet cependant pas encore d'exploiter au mieux les données, les tableaux étant bien souvent situés hors écran sans possibilité de les repositionner. Mais gageons qu'une solution ne tardera pas à être trouvée.

Une interface programmatique standardisée dite '**MAPI**' – Monitoring **API** – a spécialement été conçue dans le cadre des projets Européen IST dans l'optique de simplifier l'écriture des applications en leur offrant une couche d'abstraction de type 'flux réseaux'. Cette interface est actuellement fonctionnelle en environnement UNIX sur la majorité des interfaces réseaux via la librairie '**libpcap**' mais aussi sur les cartes d'acquisition spécialisées dites '**DAG**' (Direct Acquisition Gathering). La librairie implémentant l'interface MAPI est disponible sur le site du réseau norvégien de la recherche **UniNett**. L'image d'un environnement LOBSTER prêt à l'emploi de type '**LiveCD**' est par ailleurs proposée au téléchargement sur le site institutionnel du projet.

http://www.ist-lobster.org

Contrairement au réseau de détection '**LOBSTER**' assurant la surveillance du trafic 'normal' circulant sur l'Internet, le réseau '**NOAH**' a pour objet l'étude du trafic 'périphérique' établi avec la partie dite 'sombre' de l'Internet car constituée de systèmes non connus utilisant des adresses non déclarées. Pour cela, des systèmes de type 'pots de miel' sont utilisés qui jouent le rôle de 'leurres' permettant ainsi de collecter une information autrement inaccessible. Afin de disposer d'une surface de collecte maximale, un kit logiciel destiné à être installé sur des systèmes personnels devrait bientôt être mis à disposition de tous via le projet '**HoneyAtHome**'. Toute activité anormale laissant supposer qu'une tentative d'attaque est en cours pourra ainsi être immédiatement redirigée vers les pots de miels du réseau '**NOAH**' lesquels seront chargés de l'analyse.

http://www.fp6-noah.org/

L'article intitulé '**Building an Effective Early Warning System**' est consacré aux précautions à respecter avant toute mise en place d'une infrastructure d'alerte. L'auteur y décline les huit étapes qui, si elles sont respectées, devraient permettre une mise en œuvre efficace. Une version plus complète de l'article est mise à disposition sur le site de la société Suisse '**CyTrap Labs**', spécialisée dans l'analyse des risques.

http://www.cytrap.eu/files/EU-IST/2007/pdf/2007-01-31-ENISAQuarterly-V3-Nr1-LongVersion.pdf

Trois autres articles méritent une lecture approfondie:

- l'article '**An Introduction to SCADA Security**' qui traite d'un thème considéré comme critique depuis plusieurs années par les différentes organisations américaines chargées de la protection des actifs et de la sécurité du territoire,
- l'article '**Starting up an Early Warning System in the Netherlands**' qui propose un très intéressant retour d'expérience sur la mise en place d'un système de surveillance et d'alerte avec les problèmes politiques, techniques mais aussi, et surtout, légaux qui se posent très rapidement,
- l'article '**Bulgaria Fights Cybercrime**' qui présente les résultats des mesures mises en oeuvre par l'un des derniers entrants dans la communauté Européenne, la Bulgarie, pour contrôler la cybercriminalité qui sévit sur son territoire.

Le sommaire de ce très intéressant numéro de la lettre de l'**ENISA** est reproduit ci-dessous:

Les numéros de cette revue peuvent être reçus par messagerie électronique en s'abonnant à l'adresse mentionnée sur le site institutionnel de l'**ENISA**.

- **Complément d'information**

http://www.enisa.europa.eu/doc/pdf/publications/enisa_quarterly_03_07.pdf

METHODOLOGIE

SANS SOFTWARE SECURITY INSTITUTE - SPSA

- **Description**

Fin mars, le **Sans Institute** a annoncé l'engagement d'un projet dénommé '**Secure Programming Skill Assessment**', ou **SPSA**, destiné à améliorer le niveau de sécurité dans les développements logiciels.

L'approche retenue - qui implique, selon l'annonce de presse, plus de 362 organisations, agences gouvernementales et structures d'enseignement Américaines – s'inscrit dans la suite logique des initiatives déjà engagées visant à intervenir au plus tôt dans le cycle de formation des professionnels du logiciel. Il s'agit en effet de non seulement concevoir des enseignements sur l'art de la programmation sure mais aussi de mettre en valeur la compétence acquise par ces professionnels au moyen d'une certification reconnue comme cela est déjà le cas dans d'autres métiers spécifiques de la sécurité.

Le **SANS** indique que la logique des tests permettant de mesurer cette compétence diffère de celle habituellement mise en œuvre qui valide bien souvent une parfaite connaissance livresque de l'ouvrage associé à l'examen. Il s'agira ici au professionnel de réagir et de mettre en œuvre son expérience pour identifier les erreurs de programmation dans les exemples qui lui seront proposés et pour répondre aux questions associées.

Il n'en reste pas moins qu'une parfaite connaissance des règles fondamentales pour une programmation sure est un pré-requis indispensable à la réussite. Pour cela, et en pratique, des guides sont mis à disposition dont l'organisation thématique – laquelle s'appuie sur le concept de tâches - sera reprise dans la structuration des tests.

Quatre guides correspondant aux quatre certifications proposées sont – ou seront - disponibles sur simple demande:
- Examen langages **C** et **C++**,
- Examen langages **Java** et **J2EE**,
- Examen langage .**NET** et environnement **ASP**,
- Examen langages **PHP** et **Perl**,

Il est annoncé que les examens pourront commencer dès que la base de questions aura atteint un volume suffisant – 1200 questions pour chaque certification – pour éviter tout risque de fraude. La durée moyenne d'un examen sera de l'ordre de 3 à 5 heures dans le cas des sessions certifiantes dont la toute première est planifiée pour le mois d'août à Washington. Il est par ailleurs prévu que ces examens puissent être mis en œuvre au sein d'une entreprise comme moyen de suivi des qualifications sans qu'aucune certification ne soit cependant délivrée. Un accès ouvert sur le portail du **SANS-Sofware Security Institute** permettra à quiconque de vérifier ses compétences.

Outre les documents de présentation du projet '**SPSA**' et les exemples d'examen, nos lecteurs trouveront sur ce site un intéressant article sur les erreurs de programmation recensées par le SANS comme étant à l'origine de plus de 85% des vulnérabilités critiques trouvées à ce jour:

- **Erreur 1**: Accepter des données de la part des utilisateurs sans aucune validation ni nettoyage de celles-ci,
- **Erreur 2**: Autoriser les données destinées à être stockées dans des buffers à dépasser la taille allouée à ceux-ci,
- **Erreur 3**: Ne pas gérer correctement les entiers

On notera qu'à l'exception de la première, ces erreurs sont majoritairement le fait de la 'permissivité' de certains langages dont les langages '**C**' et '**C++**'. Extrêmement simples à décrire, ces erreurs restent cependant très difficiles à déterrer, à éradiquer, voire même simplement à éviter quand le langage employé n'embarque nativement aucun

mécanisme de protection. Si l'intégration d'outils de validation et de simulation dans les ateliers de génie logiciel peut réduire notablement les erreurs les plus grossières, il est de fait que seule la formation des développeurs aux pièges propres à chaque langage ET environnement leur permettra d'acquérir les 'bons réflexes' et de produire un code fiable dès le premier jet.

- **Complément d'information**

http://www.sans-ssi.org/ - Le portail SANS-SSI
http://www.sans-ssi.org/ssi_press.pdf - Annonce de presse
http://www.sans-ssi.org/top_three.pdf - Les trois premières erreurs de programmation selon le SANS
https://www.sans-ssi.org/blueprints.php?id=a00e5eb0973d2463632-cfcd208495d565ef602 - Guides C/CC++
https://www.sans-ssi.org/blueprints.php?id=ef8446f35513a8d3632-c4ca4238a0b92382007 - Guides Java/J2EE

SERVICES DE SECURITE

DCSSI – CATALOGUE DES PRODUITS QUALIFIES V4.2

- **Description**

La **DCSSI** vient de publier la version 4.2 de son 'catalogue des produits qualifiés'. Celui-ci recense les produits dits 'd'usage général' qualifiés ou en cours de qualification conformément à une certification de type '**Critère Communs**', à une qualification établie en référence à l'un des trois niveaux définis par la **DCSSI** (standard, renforcé ou élevé) ou encore à un agrément ou à une caution jugeant de l'aptitude à assurer la protection d'informations classifiées ou d'informations sensibles.

La liste complète des produits certifiés au titre du décret 2002-535, relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des **TI**, est publiée séparément sur le site du **SSI**.

Les produits recensés dans cette nouvelle édition du catalogue sont au nombre de 16 (contre 14 dans la version 4.1 , 13 dans la version 4.0 et 16 dans les versions 3.0 et 2.4 du catalogue):

Produit	Editeur	Certification	Qualification	Catégorie	C/Q	V4.2
Security Crypto Box	MSI	EAL4+ élevé	Standard	Ressources Cryptographiques	V2.1	
TrustWay PCI	BULL	EAL4+ élevé	Elevé	Ressources Cryptographiques	V2.2	
SecPHONE	ERCOMM	EAL2+	Standard	Ressources Cryptographiques	V4.0	
Fast	ARKOON	EAL2+	Standard	Firewall	V2.2	
Fox V3.2.6	Thalès	E4 moyen		Firewall	-	
NETASQ IPS V5	NETASQ	EAL2+	Standard	Chiffrement IP	V2.4	
M>Tunnel V2.5	EADS	EAL2+	Standard	Chiffrement IP	-	
Mistral	THALES	EAL3+	Standard	Chiffrement IP	V3.0	
TrustWay VPN	BULL	EAL2+	Standard	Chiffrement IP	V2.1	
Applatoo	FT	EAL2+	Standard	Signature	V3.0	
Adsignerweb V3.1.800	DICTAO	EAL3+	Standard	Signature	V4.1	
Fast Signature	CdC	EAL2+ visé	En cours	Signature	V4.0	
Validation Server	Dictao	EAL3 + visé	En cours	Signature	V4.1	
ZoneCentral	PRIMX	EAL2+ visé	En cours	Protection du poste de travail	V4.0	
Security Management	Exaprotect	EAL2+ visé	En cours	Administration de la sécurité	**V4.2**	**N**
OmniPCX Enterprise	Alcatel	EAL2+ visé	En cours	Voix sécurisée		**N**

Légende: **C**: Obtention de la certification **Q**: Obtention de la qualification **D**: Disparu
T: Changement de TOE **N**: Nouvel entrant

Aucune nouvelle certification n'a été délivrée depuis novembre dernier mais l'évaluation de deux nouveaux produits a été engagée. Le catalogue s'enrichit à cette occasion de deux nouvelles catégories de produits: '**Administration de la sécurité**' et '**Voix sécurisée**'.

Trois nouveaux documents ont été ajoutés au référentiel documentaire:
- la mise à jour d'un guide de 69 pages référencé '**2741/SGDN/DCSSI/SDS/LCR**' et intitulé '**Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques de niveau de robustesse standard**',
- un document de 28 pages intitulé '**Fournitures nécessaires à l'analyse de mécanismes cryptographiques**' et référencé '**2336/SGDN/DCSSI/SDS**',
- la version 3.1 révision 1 en langue anglaise des trois volets des '**Critères Communs**':
  partie 1: Introduction et modèle général - *Introduction and general model* (septembre 2006 - 86 pages),
  partie 2: Exigences fonctionnelles de sécurité - *Security functional components* (septembre 2006 - 314 pages),
  partie 3: Exigences d'assurance de sécurité - *Security assurance components* (septembre 2006 - 231 pages).

On notera que la version téléchargeable du catalogue sous la forme d'un fichier d'archive au format 'ZIP' ne semble plus être disponible.

- **Complément d'information**

http://www.ssi.gouv.fr/fr/politique_produit/catalogue/index.html - Présentation du catalogue
http://www.ssi.gouv.fr/fr/politique_produit/catalogue/pdf/CCpart1v3.1r1.pdf - CC 3.1 Rev 1 Partie 1
http://www.ssi.gouv.fr/fr/politique_produit/catalogue/pdf/CCpart2v3.1r1.pdf - CC 3.1 Rev 1 Partie 2
http://www.ssi.gouv.fr/fr/politique_produit/catalogue/pdf/CCpart3v3.1r1.pdf - CC 3.1 Rev 1 Partie 3

DCSSI – REGLES CONCERNANT LE CHOIX ET LE DIMENSIONNEMENT DES MECANISMES CRYPTOGRAPHIQUES

- **Description**

La dernière version du catalogue des produits qualifiés édité par la **DCSSI** annonce la mise à disposition d'une nouvelle version du document de référence intitulé '**Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques de niveau de robustesse standard**'. Celui-ci complète le document intitulé '**Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques de niveau de robustesse standard**' publié en novembre dernier (Rapport N°100 – Novembre 2006). Ici encore, la version diffusée – version 1.10 datée du 19 décembre 2006 et référencée N°2741/SGDN/DCSSI/SDS/LCR – est volontairement restreinte aux dispositifs du premier niveau de sécurité, dit '**standard**', sur une échelle établie par la **DCSSI** qui en comporte trois. Deux autres versions classifiées du document existent qui intègrent les deux niveaux de sécurité suivants dits '**renforcé**' et '**élevé**'.

Après un rappel des principes généraux relatifs à la définition du niveau de robustesse d'un algorithme de chiffrement et du lien entre ce niveau et de celui de la classification de l'information traitée, le guide aborde les règles et les recommandations applicables au choix de l'algorithme.

Ces règles fixent notamment le nombre d'opérations de calcul requises pour attaquer un algorithme en fixant une échéance de durée de vie: 2010 voire 2020 dans certains cas:

- Dans le cas de l'utilisation de clefs symétriques, ces limites sont fixées à 2^80 opérations avant 2010 et 2^100 après.
- Pour les algorithmes à clefs publiques, elles sont définies en imposant la taille du modulo: 1536 bits pour une échéance en 2010, 2048 bits pour 2020 et 4096 bits au-delà.
- Dans le cas des algorithmes à base de courbes elliptiques, la taille du nombre premier générateur du sous-groupe est positionnée respectivement à 160 bits et 256 bits valeurs par ailleurs aussi applicables à la taille minimale d'un condensé cryptographique.

Ces préconisations sont en accord avec les prescriptions du document précité concernant la gestion des clefs et avec l'état de l'art dont une excellente synthèse est proposée chaque année dans le rapport '**Yearly Report on Algorithms and Key Lengths**' du projet Européen **E-Crypt** (Rapport N°104 – Mars 2007).

Chaque règle, ou recommandation, est détaillée puis justifiée en respectant une convention de nommage permettant d'identifier immédiatement la nature du principe (mandataire avec le préfixe **Règle** ou discrétionnaire avec le préfixe **Recom** et un texte de description en caractères italiques) ainsi que son niveau d'application (initiale du niveau de sécurité inscrit en indice du préfixe). Dans le cas de ce document, n'apparaîtront donc que les principes de type '$Règle_s$' ou '$Recom_s$'.

La table des matières de ce document de 69 pages est présentée ci-dessous en rappelant le nombre de règles et de recommandations associées à la sélection de chacune des catégories d'algorithme.

Les chapitres annexes '**E**', '**F**' et '**G**' contiennent un grand nombre d'informations pratiques dont un glossaire des termes usités dans le domaine, une excellente présentation des différentes classes d'algorithmes et de leur spécificité ainsi qu'un intéressant état de l'art en matière d'attaques et de procédés de factorisation.

- **Complément d'information**

http://www.ssi.gouv.fr/fr/politique_produit/catalogue/pdf/mecanismes_cryptographique_v1_10_standard.pdf - Guide

REFERENCES

CIS - CATALOGUE DE PROCEDURES ET DE TESTS

- **Description**

Le **CIS** – **Center for Internet Security** – vient d'annoncer la mise à disposition des recommandations concernant la version **2005** de l'environnement de gestion de bases de données **SQL Server**.

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
HP-UX	P1	V1.3.1	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	V2.1.1	Outil publié
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	P1 P2	V1.6	Outil existant
Oracle base de donnée 8i	P1 P2	V1.1	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
N **Microsoft SQL Serveur 2005**	**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**

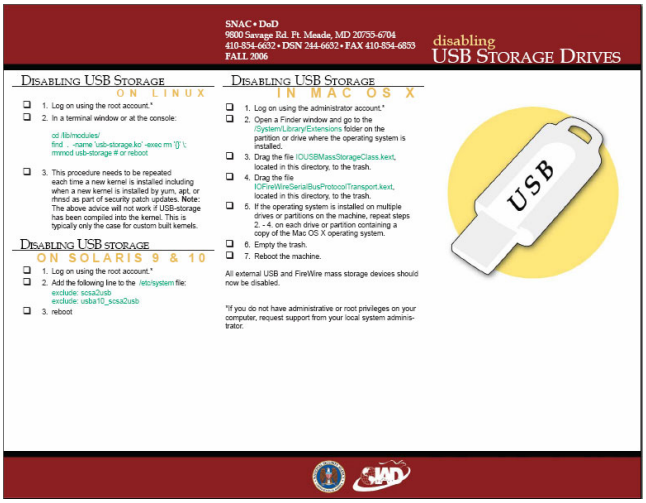
http://www.cisecurity.org/ - Accès aux tests et outils associés
http://www.cisecurity.org/bench_sqlserver.html - Procédures Niveaux 1 et 2 SQL Server 2005
http://www.cisecurity.org/tools2/sqlserver/CIS_SQL2005_Benchmark_v1.0.pdf - Catalogue

METHODE

NSA - DISABLING USB STORAGE DRIVES

- **Description**

La **NSA** a publié un nouveau mémento dans sa série des documents dits 'd'application'. Intitulé '**Disabling USB Storage Drives**', celui-ci prend la forme d'un feuillet couleur de deux pages qui décrit pas à pas les procédures à suivre pour désactiver l'accès aux medias de stockage connectés en **USB**. Sont ainsi traités les cas des systèmes d'exploitation **LINUX**, **SOLARIS 9** et **10**, **Mac OS X** et **Windows**.



Quelque soit le système, la procédure a pour objet d'invalider le chargement du code assurant la gestion des périphériques de stockage via l'interface **USB**: module noyau dynamiquement chargeable '*usb_storage.ko*' pour **LINUX**, gestionnaire de périphérique '*scsa2usb*' dans le cas de **Solaris**, modules '*IOUSBMassStorageClass.Kext*' et '*IOFireWireSerialBusProtocolTransport.kext*' pour **Mac OX X** et enfin désactivation du service '*UsbStor*' via la base de registre pour le système **Windows**.

Les conséquences de ces modifications diffèrent selon les systèmes: dans le cas des systèmes **LINUX** et **Mac OS X**, la destruction des modules gérant le stockage **USB** mais aussi **FireWire** pour Mac OS X est préconisée rendant les modifications effectuées irréversibles.

Ce n'est par contre pas le cas en ce qui concerne les systèmes **Solaris** et **Windows** où la seule solution proposée consiste en une modification du paramétrage.

Le cas des autres systèmes de la famille **BSD** n'est pas traité mais la manipulation sera similaire à celle proposée pour le système **Solaris**, à savoir la modification du paramétrage du noyau. Les opérations associées requièrent toutes de disposer de privilèges avancés, et dans certains cas, de réinitialiser préalablement le niveau de sécurité du noyau. Cette approche est une alternative simple à la mise en œuvre de logiciels de contrôle d'accès aux périphériques USB lesquels offrent cependant une bien plus grande souplesse de configuration.

- **Complément d'information**

http://www.nsa.gov/snac/support/I731-002R-2007.pdf - Disabling USB Storage Drives

REFERENCES

NSA - CATALOGUE DES GUIDES DE SECURITE

- **Description**

La **NSA** a publié un nouveau mémento portant sur la désactivation des interfaces USB pour **les périphériques de stockage de masse**.

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 2003					
	R	The Windows Server 2003 - Security Guide	V2.1	26/04/2006	MIC
N	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
M	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
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
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/I731-002R-2007.pdf - Disabling USB Storage Drives

DISA – GUIDES ET CHECKLISTS DE SECURISATION

- **Description**

La **DISA** a publié les mises à jour des guides de sécurisation des environnements de type '**ERP**' et '**Desktop**'.Un guide et une liste de contrôle concernant **les architectures collaboratives** et les outils associés dont la messagerie instantanée ont été publiés.

[3 Mise(s) à jour, 2 Nouveau(x) document(s)]

		STIG			Checklist			
APPLICATIONS								
Applications	(Services)	1.1	17/01/06	PDF	2.1.9	21/11/06	PDF	
ESM		1.1	05/06/06	PDF				
ERP	**(PeopleSoft, SAP)**	**1.1**	07/12/06	PDF	1.0	01/06/06	DOC	**M**
Database	(Générique + Oracle, SQL Server)	7.2	30/11/05	PDF	7.2.1	30/06/06	ZIP	
VoIP		2.2	21/04/06	PDF	2.2.2	19/05/06	PDF	
ENVIRONNEMENTS								
Access Control		1.1	05/06/06	PDF				
Active Directory Service		1.1	10/03/06	PDF	1.1.3	21/11/06	PDF	
Collaboration	**(environnements collaboratifs)**	1.1	28/03/07	ZIP	1.1	28/03/07	DOC	**N**
Desktop		**3.1**	09/03/07	**PDF**	**3.1.1**	19/04/07	DOC	**M**
Enclave	(Périmètre)	3.1	28/07/05	PDF	3.1.6	09/07/06	PDF	
.NET	(Draft)				1.2	28/04/06	DOC	
Secure Remote Computing		1.2	10/08/05	DOC				
PERIPHERIQUES RESEAUX								
Sharing peripheral across the network		1.1	29/07/05	PDF				
- Multi-Function Device (MFD) and Printer Checklist					1.1.2	14/04/06	PDF	
- Keyboard, Video, and Mouse (KVM) Switch Checklist					1.1.2	14/04/06	PDF	
- Storage Area Network (SAN) Checklist					1.1.3	19/05/06	PDF	
- Universal Serial Bus (USB) Checklist					1.1.2	06/04/06	PDF	
RESEAU								
Network		6.4	16/12/05	PDF	6.4.4	21/07/06	PDF	
Cisco	(Supplément)				6.1	02/12/05	PDF	
Juniper	(Supplément)				6.4	02/12/05	PDF	
IP WAN					2.3	12/08/04	PDF	
Wireless	(Liste de contôle générique)	5.1	20/02/07	PDF	5.1.1	20/02/07	PDF	
	(Liste de contôle dédiée BlackBerry)				5.1.1	20/02/07	PDF	
Wireless LAN Security Framework Addendum		2.1	31/10/05	PDF				
Wireless LAN Site Survey Addendum		1.1	31/10/05	PDF				
Wireless LAN Secure Remote Access Addendum		1.1	31/10/05	PDF				

Wireless Mobile Computing Addendum	1.1	31/10/05	PDF				
SERVICES							
DNS	3.1	19/09/06	PDF	3.1	15/03/07	PDF	
Web Servers (Générique + IIS, Netscape, Apache)	6.1	11/12/06	PDF	6.1.1	01/07	ZIP	
SYSTEMES							
OS/390 & z/OS	5.2	19/09/06	PDF	5.1.2	23/03/07	DOC	
OS/390 Logical Partition	2.2	04/03/05	PDF	2.1.4	04/06	DOC	
OS/390 RACF				5.2.2	23/03/07	DOC	
OS/390 ACF2				5.2.2	23/03/07	DOC	
OS/390 TSS				5.2.1	23/03/07	DOC	
MacOS X	1.1	15/06/04	PDF	1.1.3	28/04/06	DOC	
TANDEM	2.2	04/03/05	PDF	2.1.2	17/04/06	DOC	
UNISYS	7.2	28/08/06	PDF	7.1.2	17/04/06	PDF	
UNIX	5.1	28/03/06	PDF	5.1.5	15/03/07	DOC	
VM IBM	2.2	04/03/05	PDF	2.1.2	04/06	DOC	
SOLARIS (2.6 à 2.9)				-	20/01/04	DOC	
VMS VAX				2.2.3	17/04/06	DOC	
Windows 2000				5.1.9	30/03/07	ZIP	
Windows 2003				5.1.9	30/03/07	ZIP	
Windows XP	1.8	12/01/03	PDF	5.1.9	30/03/07	ZIP	
Windows NT	3.1	26/12/02	DOC	4.1.21	28/07/06	DOC	
Windows NT/2000/XP Addendum	5.1	21/09/05	PDF				
TECHNOLOGIES							
Biométrie	1.3	10/11/05	PDF	1.3.1	31/10/05	DOC	
SPECIFIQUE DoD							
Backbone transport	1.1	05/06/06	PDF	1.1.1	18/01/07	PDF	R
Defense switch network	2.3	30/04/06	PDF	2.3.2	01/05/06		R
Secure telecommunication Red switch network	1.1	26/03/06	PDF				R
DODI 8500.2 IA				1.1.1	18/01/07	PDF	R

N Nouveau M Mis à jour R Accès restreint

- **Complément d'information**

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

LOGICIELS LIBRES

LES SERVICES DE BASE

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

RESEAU

Nom	Fonction	Ver.	Date	Source
BIND	Gestion de Nom (DNS)	9.4.0	02/07	http://www.isc.org/
		8.4.7	21/12/05	
DHCP	Serveur d'adresse	3.0.5	11/06	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	2006g	02/04/07	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	01/04/07	ftp://ftp.sendmail.org/pub/sendmail/

WEB

Nom	Fonction	Ver.	Date	Source
APACHE	Serveur WEB	1.3.37	27/07/06	http://httpd.apache.org/dist
		2.0.59	27/07/06	
		2.2.4	06/01/07	
ModSSL	API SSL Apache 1.3.37	2.8.28	28/08/06	http://www.modssl.org
MySQL	Base SQL	5.1.17	04/04/07	http://dev.mysql.com/doc/refman/5.1/en/news.html
SQUID	Cache WEB	2.6s12	20/03/07	http://www.squid-cache.org

AUTRE

Nom	Fonction	Ver.	Date	Source
FreeRadius	Gestion de l'identité	1.1.6	12/04/07	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	2.3.35	09/04/07	ftp://ftp.openldap.org/pub/OpenLDAP/openldap-release/
Samba	Gestion de fichiers	3.0.24	05/02/07	http://us1.samba.org/samba/
Tor	Anonymat	0.1.2.13	23/04/07	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	4.4.6	01/03/07	http://www.php.net/downloads.php
		5.2.1	08/02/07	

ANALYSE RESEAU

Nom	Fonction	Ver.	Date	Source
Dsniff	Boîte à outils	2.3	17/12/00	http://www.monkey.org/~dugsong/dsniff
EtterCap	Analyse & Modification	0.7.3	29/05/05	http://ettercap.sourceforge.net/index.php?s=history
Ethereal	Analyse multiprotocole	0.99.5	01/02/07	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/ssw/
TcpDump	Analyse multiprotocole	3.9.5	19/09/06	http://www.tcpdump.org/
Libpcap	Acquisition Trame	0.9.5	19/09/06	http://www.tcpdump.org/
TcpFlow	Collecte données	0.21	07/08/03	http://www.circlemud.org/~jelson/software/tcpflow/

WinPCap	Acquisition Trame	4.0	30/01/07	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	0.9.9rc4	23/04/07	http://www.ossim.net/
SnortSnarf	Analyse Snort	050314.1	05/03/05	http://www.snort.org/dl/contrib/data_analysis/snortsnarf/
WebAlizer	Journaux serveur http	2.01-10	24/04/02	http://www.mrunix.net/webalizer/download.html

ANALYSE DE SECURITE

Nom	Fonction	Ver.	Date	Source
BackTrack	Boîte à outils	2.0	06/03/07	http://www.remote-exploit.org/backtrack_download.html
curl	Analyse http et https	7.16.2	11/04/07	http://curl.haxx.se/
FIRE	Boîte à outils	0.4a	14/05/03	http://sourceforge.net/projects/biatchux/
Nessus	Vulnérabilité réseau	2.2.9	30/10/06	http://www.nessus.org
		3.0.5	17/01/07	http://www.nessus.org
Helix	Boîte à outils	1.8	06/10/06	http://www.e-fense.com/helix/
Nikto	Analyse http et https	1.36	15/02/07	http://www.cirt.net/nikto/
nmap	Vulnérabilité réseau	4.20	11/12/06	http://www.insecure.org/nmap/nmap_changelog.html
Saint	Vulnérabilité réseau	6.4.4	16/04/07	http://www.saintcorporation.com/resources/updates.html
Sara	Vulnérabilité réseau	7.3.3	04/07	http://www-arc.com/sara/
Wikto	Analyse http et https	1.63.1	29/03/06	http://www.sensepost.com/research/wikto/
Whisker	LibWhisker	2.4	03/07	http://www.wiretrip.net/rfp/lw.asp

CONFIDENTIALITE

Nom	Fonction	Ver.	Date	Source
GPG	Signature/Chiffrement	2.0.3	08/03/07	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

CONTROLE D'ACCES RESEAU

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

CONTROLE D'INTEGRITE

Nom	Fonction	Ver.	Date	Source
RootKit hunt	Compromission UNIX	1.2.7	24/05/05	http://www.rootkit.nl
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

DETECTION D'INTRUSION

Nom	Fonction	Ver.	Date	Source
P0f	Identification passive	2.0.8	06/09/06	http://lcamtuf.coredump.cx/p0f.shtml
Snort	IDS Réseau	2.6.1.4	03/04/07	http://www.snort.org/dl/
Shadow	IDS Réseau	1.8	30/04/03	http://www.nswc.navy.mil/ISSEC/CID/

GENERATEURS DE TEST

Nom	Fonction	Ver.	Date	Source
NetDude &all	Rejeu de paquets	0.4.7	16/11/06	http://netdude.sourceforge.net/download.html
Scapy	Génération de paquet	1.0.5.20	12/12/06	http://www.secdev.org/projects/scapy/files/scapy.py

PARE-FEUX

Nom	Fonction	Ver.	Date	Source
DrawBridge	PareFeu FreeBsd	4.0	23/04/04	http://drawbridge.tamu.edu
IpFilter	Filtre datagramme	4.1.19	02/07	http://coombs.anu.edu.au/ipfilter/ip-filter.html
NetFilter	Pare-Feu IpTables	1.3.7	04/12/06	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	4.6	09/03/07	http://www.openssh.com/
OpenSwan	Pile IPSec	2.4.7	14/11/06	http://www.openswan.org/code/
PuTTY	Terminal SSH2	0.59	24/01/07	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 **29/03/2007** au **27/04/2007**, **28 RFC** ont été publiés dont 9 RFC ayant trait à la sécurité.

RFC TRAITANT DE LA SÉCURITÉ

Thème	Num	Date	Etat	Titre
CMS	4853	04/07	Pst	Cryptographic Message Syntax (CMS) Multiple Signer Clarification
FTP	4823	04/07	Inf	FTP Transport for Secure Peer-to-Peer Business Data Interchange over the Internet
IP	4840	04/07	Inf	Multiple Encapsulation Methods Considered Harmful
IPSEC	4835	04/07	Pst	Cryptographic Algorithm Implementation Requirements for ESP and Authentication Header (AH)
IPV6	4843	04/07	Exp	An IPv6 Prefix for Overlay Routable Cryptographic Hash Identifiers (ORCHID)
	4877	04/07	Pst	Mobile IPv6 Operation with IKEv2 and the Revised IPsec Architecture
iSCSI	4850	04/07	Pst	Declarative Public Extension Key for iSCSI Node Architecture
NETLMM	4832	04/07	Inf	Security Threats to Network-Based Localized Mobility Management (NETLMM)
RADIUS	4818	04/07	Pst	RADIUS Delegated-IPv6-Prefix Attribute

RFC TRAITANT DE DOMAINES CONNEXES A LA SECURITE

Thème	Num	Date	Etat	Titre
CRYPTO	4814	03/07	Inf	Hash and Stuffing: Overlooked Factors in Network Device Benchmarking
MPLS	4817	03/07	Pst	Encapsulation of MPLS over Layer 2 Tunneling Protocol Version 3

AUTRES RFC

Thème	Num	Date	Etat	Titre
DHCP	4833	04/07	Pst	Timezone Options for DHCP
INFO	4810	03/07	Inf	Long-Term Archive Service Requirements
	4838	04/07	Inf	Delay-Tolerant Networking Architecture
	4879	04/07	BCP	Clarification of the Third Party Disclosure Procedure in RFC 3979
IPV6	4852	04/07	Inf	IPv6 Enterprise Network Analysis - IP Layer 3 Focus
MPLS	4829	04/07	Inf	Label Switched Path (LSP) Preemption Policies for MPLS Traffic Engineering
NETLMM	4830	04/07	Inf	Problem Statement for Network-Based Localized Mobility Management (NETLMM)
	4831	04/07	Inf	Goals for Network-Based Localized Mobility Management (NETLMM)
OPF	4839	04/07	Inf	Media Type Registrations for the Open eBook Publication Structure (OEBPS) Package File (OPF)
PPVPN	4834	04/07	Inf	Requirements for Multicast in Layer 3 Provider-Provisioned Virtual Private Networks (PPVPNs)
RSVP	4859	04/07	Inf	Codepoint Registry for the Flags Field in RSVP-TE Session Attribute Object
	4874	04/07	Pst	Exclude Routes - Extension to Resource ReserVation Protocol-Traffic Engineering (RSVP-TE)
RTP	4867	04/07	Pst	RTP Payload Format and File Storage Format for AMR and AMR-WB Audio Codecs
SCTP	4820	03/07	Pst	Padding Chunk and Parameter for the Stream Control Transmission Protocol (SCTP)
SDH	4842	04/07	Pst	Synchronous Optical Network/Synchronous Digital Hierarchy (SONET/SDH) CEP
TCP	4821	03/07	Pst	Packetization Layer Path MTU Discovery
	4828	04/07	Exp	TCP Friendly Rate Control (TFRC): The Small-Packet (SP) Variant

LES DRAFTS

Du **29/03/2007**au **27/04/2007**, 182 drafts ont été publiés : **129** drafts mis à jour, **53** nouveaux drafts, dont **31** drafts ayant directement trait à la sécurité.

NOUVEAUX DRAFTS TRAITANT DE LA SECURITE

Thème	Nom du Draft	Date	Titre
AUTH	draft-josefsson-password-auth-00	28/03	A Password-based Authentication Protocol
DNS	draft-wijngaards-dnsext-trust-history-00	20/04	DNSSEC Trust Anchor History Service
	draft-moreau-srvloc-dnssec-priming-00	20/04	DNSSEC Validation Root Priming Through SLP (DNSSEC-ROOTP)
TLS	draft-badra-tls-password-00	20/04	Password Ciphersuites for Transport Layer Security (TLS)
	draft-badra-tls-password-ext-00	20/04	Password Extension for TLS Client Authentication
	draft-ietf-tls-suiteb-00	23/04	Suite B Cipher Suites for TLS
	draft-ietf-tls-ecc-new-mac-00	23/04	TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES GCM

MISE A JOUR DE DRAFTS TRAITANT DE LA SECURITE

Thème	Nom du Draft	Date	Titre
DTNRG	draft-irtf-dtnrg-bundle-security-03	24/04	Bundle Security Protocol Specification
EAP	draft-funk-eap-ttls-v0-01	20/04	EAP Tunneled TLS Authentication Protocol Version 0 (EAP-TTLSv0)
INCH	draft-ietf-inch-iodef-12	26/04	The Incident Object Description Exchange Format

IP	draft-meghana-mip4-mobike-optimizations-02	20/04	Optimizations to Secure Connectivity and Mobility
ISIS	draft-ietf-isis-hmac-sha-02	10/04	IS-IS Generic Cryptographic Authentication
KRB	draft-richards-otp-kerberos-02	16/04	OTP Kerberos
MEDIA	draft-wing-media-security-requirements-02	20/04	Media Security Requirements
MIKEY	draft-ietf-msec-mikey-ecc-02	28/03	ECC Algorithms for MIKEY
OPENPGP	draft-ietf-openpgp-rfc2440bis-22	25/04	OpenPGP Message Format
OPSEC	draft-ietf-opsec-infrastructure-security-01	10/04	Service Provider Infrastructure Security
PKIX	draft-pinkas-pkix-lcvp-01	18/04	Lightweight Certificate Validation Protocol (LCVP)
	draft-ietf-sidr-res-certs-06	10/04	A Profile for X.509 PKIX Resource Certificates
RADIUS	draft-ietf-mip4-radius-requirements-02	25/04	Mobile IPv4 RADIUS requirements
	draft-zorn-radius-logoff-09	17/04	User Session Tracking in RADIUS
	draft-zorn-radius-err-msg-07	17/04	RADIUS Error Messages
	draft-zorn-radius-keyreq-07	17/04	Session Key Transport in RADIUS
	draft-zorn-radius-keywrap-13	17/04	RADIUS Attributes for the Delivery of Keying Material
	draft-zorn-radius-encattr-06	18/04	Transmitting Confidential Data in RADIUS
	draft-ietf-radext-fixes-03	10/04	Common RADIUS Implementation Issues and Suggested Fixes
	draft-ietf-radext-rfc3576bis-04	11/04	Dynamic Authorization Extensions to RADIUS
SASL	draft-ietf-sasl-gs2-08	29/03	Using GSS-API Mechanisms in SASL: The GS2 Mechanism Family
SMIME	draft-ietf-smime-cms-auth-enveloped-04	26/04	CMS Authenticated-Enveloped-Data Content Type
SYSLOG	draft-ietf-syslog-transport-tls-09	23/04	TLS Transport Mapping for Syslog
TCP	draft-ietf-tcpm-syn-flood-03	20/04	TCP SYN Flooding Attacks and Common Mitigations
VMAC	draft-krovetz-vmac-01	23/04	VMAC: Message Authentication Code using Universal Hashing

DRAFTS TRAITANT DE DOMAINES CONNEXES A LA SECURITE

Thème	Nom du Draft	Date	Titre
6LOWPAN	draft-dokaspar-6lowpan-routreq-01	29/03	Design Goals and Requirements for 6LoWPAN Mesh Routing
DIAMETER	draft-fajardo-dime-app-design-guide-02	18/04	Diameter Applications Design Guidelines
EME	draft-irtf-eme-francis-nutss-design-00	23/04	An EME Signaling Protocol Design
HIP	draft-ietf-hip-dns-09	13/04	Host Identity Protocol (HIP) Domain Name System Extensions
	draft-ietf-hip-applications-01	10/04	Using the Host Identity Protocol with Legacy Applications
IETF	draft-lear-ietf-syslog-rfc3195bis-01	20/04	Reliable Delivery for syslog
IGMP	draft-vijay-magma-igmppr...-intf-learning-00	28/03	IGMP /MLD Proxy Upstream Interface Learning
IPV6	draft-ietf-netlmm-proxymip6-00	12/04	Proxy Mobile IPv6
	draft-ietf-netlmm-pmip6-ipv4-support-00	26/04	IPv4 Support for Proxy Mobile IPv6
	draft-devarapalli-netlmm-pmipv6-mipv6-01	26/04	Proxy Mobile IPv6 and Mobile IPv6 interworking
	draft-weniger-netlmm-pmipv6-...-issues-00	20/04	Proxy Mobile IPv6 and Mobile IPv6 interworking issues
L3VPN	draft-ietf-l3vpn-bgpvpn-auto-09	25/04	BGP as an Auto-Discovery Mechanism for VR-based Layer-3 VPNs
	draft-zhang-l3vpn-vr-mcast-03	13/04	Multicast in Virtual Router-based IP VPNs
	draft-mirtorabi-l3vpn-igp-transparency-00	13/04	IGP transparency of VPN routes when BGP is used as a PE-CE
LDAP	draft-zeilenga-ldap-entrydn-02	26/04	The LDAP entryDN Operational Attribute
MMUSIC	draft-ietf-mmusic-ice-15	28/03	ICE: A Methodology for NAT Traversal for Offer/Answer Protocols
MPLS	draft-vapiwala-bmwg-rsvpte-...-motivation-00	16/04	Motivation for Benchmarking MPLS TE convergence
	draft-mnapierala-mvpn-rev-01	23/04	Multicast MPLS/BGP VPNs Revisited
RRG	draft-irtf-rrg-design-goals-00	20/04	Design Goals for Scalable Internet Routing
SIP	draft-ietf-sip-fork-loop-fix-05	28/03	Addressing an Amplification Vulnerability in SIP Forking Proxies
SYSLOG	draft-gerhards-chisholm-syslog-alarm-00	16/04	Alarms in SYSLOG

AUTRES DRAFTS

Thème	Nom du Draft	Date	Titre
2822UPD	draft-resnick-2822upd-01	26/04	Internet Message Format
ATOMPUB	draft-nottingham-atompub-feed-history-09	23/04	Feed Paging and Archiving
	draft-snell-atompub-feed-license-11	28/03	Atom License Extension
AUTOCON	draft-jeong-autoconf-pdad-on-demand-01	20/04	Duplicate Address Detection for On-demand Routing Protocols
BFD	draft-shen-bfd-intf-p2p-nbr-00	28/03	Interface Based Point-to-Point Neighbor BFD
BGP	draft-rekhter-as4octet-ext-community-02	23/04	Four-octet AS Specific BGP Extended Community
CAPWAP	draft-ietf-capwap-protocol-specification-06	13/04	CAPWAP Protocol Specification
	draft-ietf-capwap-protocol-...-ieee80211-03	12/04	CAPWAP Protocol Binding for IEEE 802.11
CIDR	draft-terrell-cidr-net-....s-iptx-add-spc-16	16/04	CIDR Network Descriptor expands the size of the IPtX
DATAMOD	draft-alexan-datamod-00	28/03	NE/Facilities/Lines/Protocols/Services Modeling
DHCP	draft-ietf-dhc-vpn-option-06	17/04	Virtual Subnet Selection Option
	draft-ietf-dhc-pxelinux-01	18/04	PXELINUX Use of 'Site Local' Option Space
	draft-volz-dhc-3942-status-00	20/04	Status of Reclassifying DHCPv4 Options (RFC 3942)
	draft-dhankins-dhcp-option-guidelines-00	23/04	Guidelines for Creating New DHCP Options
	draft-calhoun-dhc-capwap-ac-option-00	25/04	CAPWAP Access Controller DHCP Option
DKIM	draft-ietf-dkim-ssp-requirements-04	23/04	Requirements for a DKIM Signing Practices Protocol
DNS	draft-iab-dns-synthesis-concerns-00	16/04	Concerns on the synthesis of non-existent names in DNS.
	draft-anderson-reverse-dns-status-00	24/04	Reverse DNS Status Report
DTN	draft-kutscher-dtnrg-uni-clayer-00	17/04	A DTN Convergence Layer Protocol for Unidirectional Transport
	draft-irtf-dtnrg-bundle-spec-09	18/04	Bundle Protocol Specification
EBU	draft-evain-ebu-urn-00	28/03	A URN Namespace for the European Broadcasting Union (EBU)
ECTP	draft-dykim-ectp-00	18/04	Enhanced Communications Transport Protocol for One-to-Many
EMAIL	draft-hathcock-minger-01	28/03	The Minger Email Address Verification Protocol
ENUM	draft-ietf-enum-iax-02	18/04	IANA Registration for IAX Enumservice
	draft-ietf-enum-unused-02	28/03	IANA Registration for Enumservice UNUSED

	draft-hoeneisen-enum-x-service-regs-00	28/03	Registration of Enumservices for experimental, private or trial use
ESDS	draft-young-esds-concepts-00	12/04	Extensible Supply-chain Discovery Service Concepts
	draft-thompson-esds-commands-00	12/04	Extensible Supply-chain Discovery Service Commands
	draft-thompson-esds-schema-00	12/04	Extensible Supply-chain Discovery Service Schema
FORCES	draft-dong-forces-lfblib-00	28/03	A LFB Library for ForCES
GEOPRIV	draft-linsner-geopriv-relativeloc-00	20/04	Relative Location for Civic Location Format
IAV	draft-iab-raws-report-02	16/04	Report from the IAB Workshop on Routing and Addressing
IAX2	draft-guy-iax-03	18/04	IAX2: Inter-Asterisk eXchange Version 2
IDLOC	draft-carpenter-idloc-map-cons-00	18/04	General Identifier-Locator Mapping Considerations
IDR	draft-ietf-idr-v4nlri-v6nh-00	28/03	Advertising an IPv4 NLRI with an IPv6 Next Hop
IETF	draft-klensin-norm-ref-04	28/03	Handling Normative References to Standards Track Documents
	draft-josefsson-free-standards-howto-00	24/04	Guidelines for Free Standards in the IETF
IMAP	draft-gulbrandsen-imap-notify-05	26/04	The IMAP NOTIFY Extension
	draft-cridland-imap-context-01	25/04	Contexts for IMAP4
IPFIX	draft-ietf-ipfix-implementation-guidelines-03	26/04	IPFIX Implementation Guidelines
	draft-ietf-ipfix-biflow-04	11/04	Bidirectional Flow Export using IPFIX
IPPM	draft-ietf-ippm-duplicate-00	18/04	A One-Way Packet Duplication Metric for IPPM
IPV4	draft-ietf-mip4-nemov4-dynamic-00	28/03	Dynamic Prefix Allocation for NEMOv4
	draft-ietf-mip4-nemov4-fa-00	28/03	FA extensions to NEMOv4 Base
IPV6	draft-ietf-mip6-bootstrapping-...-dhc-03	23/04	MIP6-bootstrapping for the Integrated Scenario
	draft-haberman-ipv6-ra-flags-option-01	18/04	IPv6 Router Advertisement Flags Option
	draft-rekhter-v6-ext-communities-01	23/04	IPv6 Address Specific BGP Extended Communities Attribute
	draft-giaretta-netlmm-mip-interactions-00	24/04	Interactions between PMIPv6 and MIPv6
	draft-ietf-v6ops-scanning-implications-03	28/03	IPv6 Implications for Network Scanning
	draft-ietf-v6ops-campus-transition-01	28/03	IPv6 Campus Transition Scenario Description and Analysis
iSCSI	draft-ietf-ips-iscsi-impl-guide-07	16/04	iSCSI Corrections and Clarifications
JABBER	draft-saintandre-jabberid-05	10/04	The Jabber-ID Header Field
LEMONAD	draft-ietf-lemonade-convert-06	12/04	IMAP CONVERT extension
	draft-ietf-lemonade-reconnect-client-04	26/04	IMAP4 Extensions for Quick Mailbox Resynchronization
MANET	draft-ietf-manet-iana-01	16/04	MANET IANA Needs
	draft-ietf-manet-jitter-00	20/04	Jitter considerations in MANETs
	draft-ietf-manet-timetlv-00	20/04	Representing multi-value time in MANETs
MATH	draft-terrell-math-quant-... -of-binary-sys-06	16/04	The Mathematics of Quantification
METRICS	draft-bradner-metricstest-01	20/04	Advancement of metrics specifications on IETF Standards Track
MGCP	draft-auerbach-mgcp-rtcpxr-06	13/04	RTCP XR VoIP Metrics Package for the MGCP
MIB	draft-combes-ipdvb-mib-rcs-00	29/03	The DVB-RCS MIB
MPLS	draft-ietf-ccamp-inter-domain-rsvp-te-06	23/04	Inter domain MPLS and GMPLS TE - RSVP-TE extensions
	draft-ietf-ccamp-lsp-stitching-06	23/04	LSP Stitching with GMPLS TE
	draft-ietf-ccamp-inter-domain-pd-path-..-05	23/04	Establishing Inter-domain TE LSPs
	draft-ietf-ccamp-gmpls-addressing-06	18/04	Use of Addresses in GMPLS Networks
	draft-ietf-ccamp-gmpls-mln-reqs-03	25/04	Requirements for GMPLS-based MRN/MLN
	draft-ietf-mpls-multicast-encaps-04	18/04	MPLS Multicast Encapsulations
MSML	draft-saleem-msml-03	20/04	Media Server Markup Language (MSML)
NEMO	draft-eddy-nemo-aero-reqs-00	12/04	NEMO Route Optimization Requirements for Operational Use
NETCONF	draft-iijima-netconf-soap-implementation-02	20/04	Experience of implementing NETCONF over SOAP
NSIS	draft-ietf-nsis-qspec-16	28/03	QoS NSLP QSPEC Template
OSPF	draft-mirtorabi-ospf-tag-04	11/04	Ext. to OSPFv2 for Advertising Optional Prefix/Link Attributes
	draft-ietf-ospf-multi-area-adj-07	28/03	OSPF Multi-Area Adjacency
	draft-ietf-ospf-dbex-opt-01	12/04	OSPF Database Exchange Summary List Optimization
	draft-ietf-pce-disco-proto-ospf-03	12/04	OSPF protocol extensions for Path Computation Element Discovery
P2P	draft-strauss-p2p-chat-07	16/04	P2P CHAT - A Peer-to-Peer Chat Protocol
PCE	draft-lee-pce-global-concurrent-opti..-03	25/04	PCECP Requirements and Protocol Extensions
PKIX	draft-ietf-pkix-lightweight-ocsp-profile-10	20/04	Lightweight OCSP Profile for High Volume Environments
PWE3	draft-ietf-pwe3-ms-pw-requirements-05	28/03	Requirements for Multi-Segment PWE3
QOS	draft-levis-provider-qos-agreement-01	29/03	provider-to-provider agreements for Internet-scale QoS
RFC2026	draft-carpenter-rfc2026-critique-03	20/04	RFC 2026 in practice
RFC2413	draft-kunze-rfc2413bis-07	25/04	The Dublin Core Metadata Element Set
RFC3920	draft-saintandre-rfc3920bis-02	18/04	XMPP: Core
RFC3921	draft-saintandre-rfc3921bis-02	18/04	XMPP: Instant Messaging and Presence
RFC4234	draft-crocker-rfc4234bis-00	24/04	Augmented BNF for Syntax Specifications: ABNF
RIF	draft-moriarty-post-inch-rid-01	11/04	Real-time Inter-network Defense
RMT	draft-ietf-rmt-fec-bb-revised-07	18/04	Forward Error Correction (FEC) Building Block
	draft-ietf-rmt-bb-fec-ldpc-05	29/03	LDPC Staircase and Triangle FEC Schemes
RPSL	draft-uijterwaal-rpsl-4byteas-ext-02	29/03	RPSL extensions for 32 bit AS Numbers
RSN	draft-culler-rsn-routing-reqs-00	13/04	Routing Requirements for Sensor Networks
RTP	draft-ietf-avt-rtp-jpeg2000-15	24/04	RTP Payload Format for JPEG 2000 Video Streams
	draft-ietf-avt-rtp-jpeg2000-beam-06	18/04	Extensions for Scalability and Main Header Recovery
	draft-ietf-avt-rtp-no-op-02	17/04	A No-Op Payload Format for RTP
	draft-ietf-avt-rtp-vorbis-03	18/04	RTP Payload Format for Vorbis Encoded Audio
	draft-ietf-dccp-rtp-05	28/03	RTP and the Datagram Congestion Control Protocol (DCCP)
	draft-wing-behave-symmetric-rtprtcp-03	16/04	Symmetric RTP/RTCP
SHIM6	draft-ietf-shim6-proto-08	23/04	Shim6: Level 3 Multihoming Shim Protocol for IPv6
SIP	draft-pailer-locpres-00	28/03	A Location Presence Event Package for SIP
	draft-linyi-sipping-invite-with-conf-info-00	13/04	Session Initiation Protocol (SIP) INVITE with Conference Info
	draft-vanelburg-sipping-served-user-00	18/04	The SIP P-Served-User Private-Header (P-Header)
	draft-ietf-sip-gruu-13	10/04	Obtaining and Using Globally Routable UA URIs (GRUU) in SIP
	draft-ietf-sip-sips-03	16/04	The use of the SIPS URI Scheme in SIP

	draft-ietf-sipping-capacity-attribute-04	28/03	XML Format Extension for Representing Copy Control Attributes
	draft-ietf-sipping-consent-format-03	25/04	A Document Format for Requesting Consent
	draft-ietf-sipping-sbc-funcs-03	18/04	Requirements from SIP Session Border Control Deployments
	draft-ietf-sipping-ipv6-torture-tests-02	23/04	SIP Torture Test Messages for Internet Protocol Version 6 (IPv6)
SIPSO	draft-stjohns-sipso-01	11/04	Son of IPSO (SIPSO) A Simple IPv6 Sensitivity Labeling Option
SMIME	draft-housley-smime-suite-b-01	25/04	Suite B in Secure/Multipurpose Internet Mail Extensions (S/MIME)
	draft-ietf-smime-escertid-05	19/04	ESS Update: Adding CertID Algorithm Agility
SMTP	draft-ietf-eai-smtpext-05	11/04	SMTP extension for internationalized email address
	draft-ietf-eai-utf8headers-05	26/04	Internationalized Email Headers
	draft-klensin-rfc2821bis-03	25/04	Simple Mail Transfer Protocol
	draft-fanf-smtp-quickstart-01	10/04	The QUICKSTART SMTP service extension
	draft-hansen-4468upd-mailesc-registry-01	11/04	A Registry for Mail Enhanced Status Codes
	draft-fanf-smtp-quickstart-a-00	18/04	The QUICKSTART SMTP service extension (simple profile)
	draft-fanf-smtp-quickstart-b-00	18/04	The QUICKSTART SMTP service extension (full profile)
SNMP	draft-schoenw-snmp-discover-02	16/04	Simple Network Management Protocol (SNMP) EngineID Discovery
SOCIAL	draft-varun-social-networking-01	28/03	An Architecture for Human Meetings and Dating websites
SPEERMI	draft-lendl-speermint-background-00	18/04	Background and Assumptions of the Speermint WG
	draft-ietf-speermint-architecture-03	24/04	SPEERMINT Peering Architecture
	draft-ietf-speermint-flows-02	24/04	SPEERMINT Routing Architecture Message Flows
TCP	draft-floyd-tcpm-ackcc-00	16/04	Adding Acknowledgement Congestion Control to TCP
TMRG	draft-irtf-tmrg-metrics-09	28/03	Metrics for the Evaluation of Congestion Control Mechanisms
TRIP	draft-carlberg-trip-attribute-rp-01	23/04	TRIP Attribute for Resource Priority
TSVWG	draft-ietf-tsvwg-admitted-realtime-dscp-01	28/03	DSCPs for Capacity-Admitted Traffic
	draft-ietf-tsvwg-cc-alt-02	26/04	Specifying New Congestion Control Algorithms
UNICODE	draft-crispin-collation-unicasemap-03	17/04	unicode-casemap - Simple Unicode Collation Algorithm
XCON	draft-ietf-xcon-common-data-model-05	18/04	Conference Information Data Model for Centralized Conferencing
XMPP	draft-saintandre-xmpp-presence-analysis-00	12/04	Interdomain Presence Scaling Analysis for XMPP

NOS COMMENTAIRES

LES DRAFTS

DRAFT-IETF-DNSOP-AS112-OPS-00

The AS112 Project

Sous le nom de code de '**Projet AS112**' se cache une infrastructure permettant de parer aux inévitables erreurs de configuration des points d'accès Internet et de venir au secours de leurs exploitants. Nul n'est sans ignorer qu'un certain nombre de blocs d'adresses **IP** ont été réservés en 1996 dans une manœuvre désespérée pour contrer l'inévitable épuisement des adresses **IP** V4 publiques. Ces adresses sont désormais connues sous le nom d'adresses '**RFC1918**' en référence au standard les ayant établies. Ce **RFC**, au nom prédestiné, aura mis fin – du moins temporairement - à la guerre à laquelle se livraient les différents acteurs présents sur l'Internet pour obtenir leur quota d'adresses.

Pour mémoire, les blocs d'adresses suivants ont été réservés à cet usage et, en conséquence, doivent impérativement être filtrés – en sortie - sur les points d'accès:

Début du bloc	Fin du bloc	Plage
10.0.0.0	10.255.255.255	10/8
172.16.0.0	172.31.255.255	172.16/12
192.168.0.0	192.168.255.255	192.168/16

L'utilisation de ces blocs d'adresses dans les réseaux internes – dits **Intranet** – a en effet, non seulement permis de minimiser le nombre d'adresses routables monopolisées, mais a aussi favorisé le déploiement du mécanisme corollaire dit de translation d'adresses ou '**NAT**'.

Nombreuses sont cependant encore les erreurs de configuration qui conduisent à transmettre notamment des requêtes DNS de résolution inverse (recherche du nom du système associé à une adresse donnée) portant sur des adresses RFC1918 vers les serveurs **DNS** centraux. Ces requêtes, pour lesquelles aucune réponse valable ne peut être fournie, génèrent une surcharge préjudiciable au bon fonctionnement de l'Internet.

Le projet **AS112** a pour objectif la mise en place de serveurs **DNS** dédiés au traitement de ces requêtes, opérés indépendamment par des volontaires et répartis de par le monde. Pour ce faire, toutes les requêtes concernant les adresses **RFC1918** sont reroutées vers un domaine de collecte (en pratique un domaine de routage autonome ou **AS**) référencé **AS112**, annoncé sur l'Internet et associé au bloc d'adresses **192.175.48.0/24**.

La proposition de standard intitulée '**The AS112 Project**' détaille les conditions techniques de mise en œuvre d'un nœud **DNS** et les contraintes opérationnelles liées à son intégration dans le système **AS112**.

Ce projet dispose d'un portail **WEB** sur lequel peuvent être trouvées toutes les informations utiles ainsi qu'une liste des volontaires – 50 à ce jour dont une majorité d'**ISP** (les Français brillent par leur absence) - ayant mis en place un routage vers les serveurs du projet **AS112**, que ce soit pour absorber le trafic généré par leurs propres utilisateurs ou pour aider à relayer le trafic en provenance d'autres réseaux.

La table des matières de cette spécification (22 pages) est reproduite ci-après :

Un second document a été publié en même temps que la proposition précédemment commentée. Intitulé '**I'm Being Attacked by PRISONER.IANA.ORG!**', ce document est plus particulièrement destiné aux exploitants des points d'accès Internet lesquels peuvent se retrouver confrontés avec des alarmes de sécurité liées à la mise en place sur l'Internet de la dite infrastructure **AS112**.

De telles alarmes peuvent être déclenchées par les réponses retournées par les serveurs **DNS** de cette infrastructure

à la suite de la réception d'une demande de résolution portant sur une adresse inscrite dans les blocs d'adresses réservés aux réseaux internes et ne devant donc normalement pas transiter sur l'Internet. L'apparition d'alarmes liées à des paquets en provenance des systèmes externes dénommés **PRISONER**, **BLACKHOLE-1** et **BLACKHOLE-2** appartenant au domaine **IANA.ORG** devra être considérée comme symptomatique d'un problème de configuration qu'il faudra rapidement solutionner et non d'une tentative d'attaque.

Les adresses affectées à ces trois systèmes sont les suivantes:
- **PRISONER.IANA.ORG** 192.175.48.1
- **BLACKHOLE-1.IANA.ORG** 192.175.48.6
- **BLACKHOLE-2.IANA.ORG** 192.175.48.42

La table des matières de ce document (17 pages) est reproduite ci-après :

http://public.as112.net/ - Portail WEB du projet AS112
ftp://ftp.isi.edu/in-notes/rfc1918.txt - Le RFC1918
ftp://ftp.nordu.net/internet-drafts/draft-ietf-dnsop-as112-ops-00.txt - Spécification AS112
ftp://ftp.nordu.net/internet-drafts/draft-ietf-dnsop-as112-under-attack-help-help-00.txt - Guide d'aide AS112

ALERTES ET ATTAQUES

ALERTES

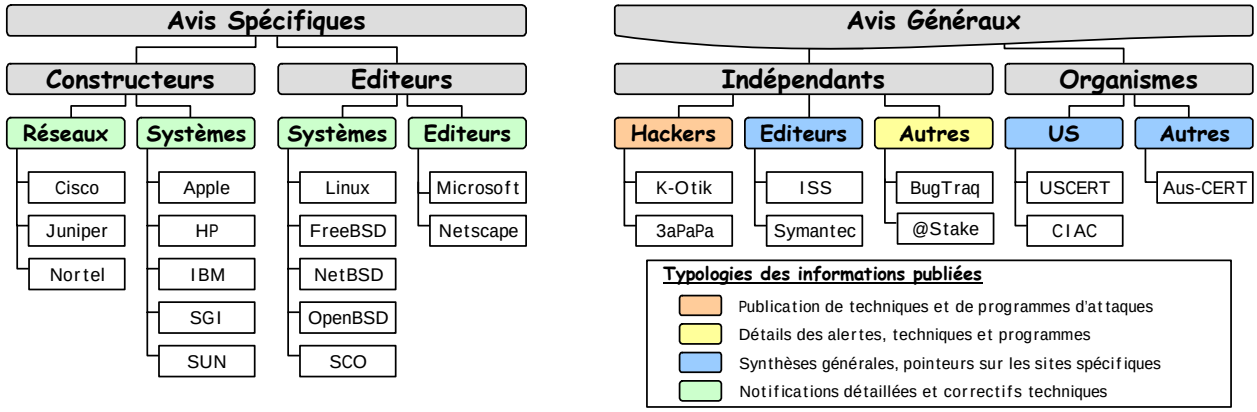
GUIDE DE LECTURE

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.

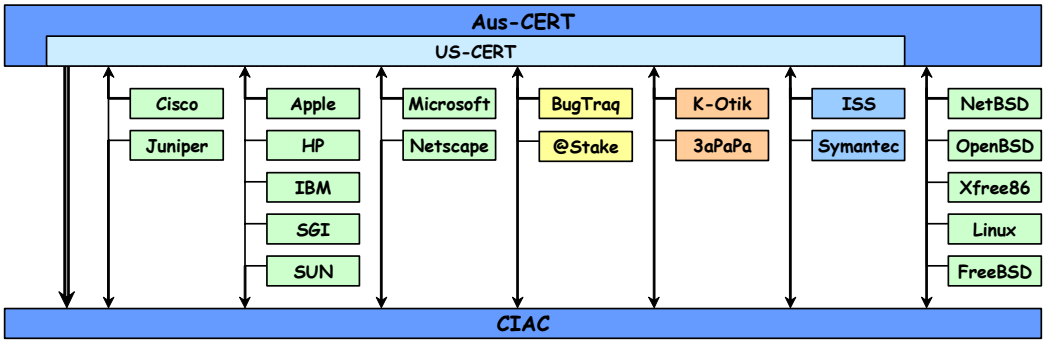
La seconde alternative, pour séduisante quelle soit, ne peut être raisonnablement mise en œuvre étant donné l'actuelle diversité des systèmes impactés. En conséquence, nous nous proposons de maintenir une synthèse des avis classée par organisme émetteur de l'avis.

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

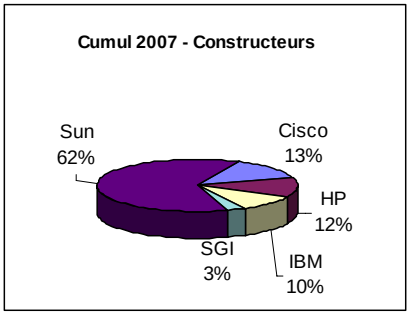
SOURCE
TITRE
Description sommaire
URL pointant sur la source d'information
Référence(s) CVE si définie(s)

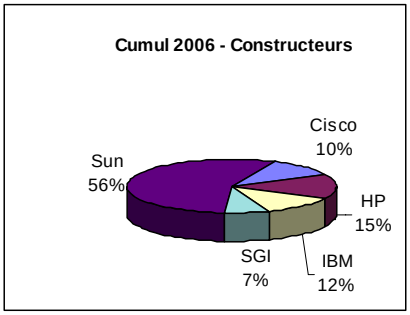
SYNTHESE MENSUELLE

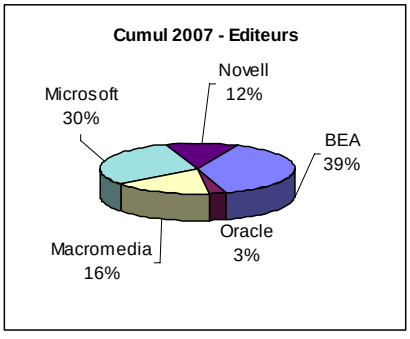
Le tableau suivant propose un récapitulatif du nombre d'avis publiés pour la période courante, l'année en cours et l'année précédente. Ces informations sont mises à jour à la fin de chaque période de veille. L'attention du lecteur est attirée sur le fait que certains avis sont repris et rediffusés par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

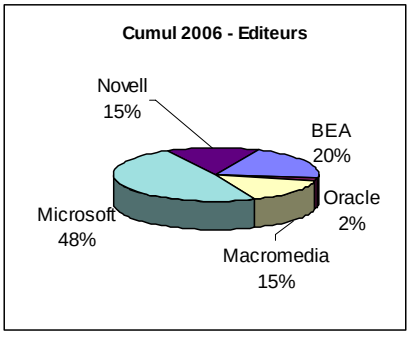
Période du **29/03/2007** au **27/04/2007**

		Cumul	
	Période	**2007**	**2006**
Organisme	**35**	**124**	**251**
US-CERT TA	7	19	39
US-CERT ST	2	8	9
CIAC	26	97	203
Constructeurs	**46**	**171**	**324**
Cisco	3	22	34
HP	6	21	49
IBM	6	17	38
SGI	1	5	22
Sun	30	106	181
Editeurs	**12**	**73**	**162**
BEA	0	28	32
Oracle	1	2	4
Macromedia	3	12	24
Microsoft	6	22	78
Novell	2	9	24
Unix libres	**71**	**324**	**994**
Linux RedHat	16	69	151
Linux Fedora	12	79	207
Linux Debian	9	43	311
Linux Mandr.	25	95	225
Linux SuSE	8	34	74
FreeBSD	1	4	26
Autres	**6**	**48**	**111**
iDefense	4	42	80
eEye	2	2	21
NGS Soft.	0	4	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

Elévation de privilèges dans 'Bridge'			
Une faille non documentée dans le produit 'Bridge' peut permettre à un utilisateur local d'élever ses privilèges.			
Forte	11/04	Adobe 'Bridge' version 1.0.3	
Correctif existant		Programme d'installation	Non disponible
Adobe		http://www.adobe.com/support/security/bulletins/apsb07-09.html	
CVE-2007-1279			

Permissions trop laxistes dans 'ColdFusion MX'			
Des permissions trop laxistes peuvent permettre à un utilisateur local malveillant d'exécuter du code arbitraire.			
Forte	11/04	Adobe 'ColdFusion MX' version 7.X sur plates-formes UNIX	
Correctif existant		Multiples fichiers et répertoires	Permissions trop laxistes
Adobe		http://www.adobe.com/support/security/bulletins/apsb07-08.html	
CVE-2007-1874			

Faille dans 'Flash Player' avec le navigateur 'Opera'			
Une faille non documentée affecte le plugin 'Flash Player' sur les plate-formes Linux, Solaris et FreeBSD.			
N/A	11/04	Adobe 'Flash Player' version 7.x et 9.x	
Correctif existant		Plugin pour 'Opera'	Non disponible
Adobe		http://www.adobe.com/support/security/advisories/apsa07-03.html	

APPLE

Multiples failles dans 'Mac OS X' et 'Mac OS X Server'			
De nombreuses vulnérabilités peuvent entraîner des dénis de service d'applications et l'exécution de code arbitraire.			
Forte	19/04	Apple 'Mac OS X' et 'Mac OS X Server' version 10.3.9 et 10.4.9	
Correctif existant		Composants	Multiples failles
Apple		http://lists.apple.com/archives/security-announce/2007/Apr/msg00001.html	
CVE-2006-0300, CVE-2006-5867, CVE-2006-6143, CVE-2006-6652, CVE-2007-0022, CVE-2007-0465, CVE-2007-0646, CVE-2007-0724, CVE-2007-0725, CVE-2007-0729, CVE-2007-0732, CVE-2007-0734, CVE-2007-0735, CVE-2007-0736, CVE-2007-0737, CVE-2007-0738, CVE-2007-0739, CVE-2007-0741, CVE-2007-0742, CVE-2007-0743, CVE-2007-0744, CVE-2007-0746, CVE-2007-0747, CVE-2007-0957, CVE-2007-1216			

Failles dans 'AirPort Extreme Base Station'			
Deux failles permettent à un attaquant distant de mener diverses attaques sur des machines du réseau local.			
Forte	09/04	Apple 'AirPort Extreme Base Station'	
Correctif existant		Support '802.11n', 'IPv6'	Erreur de configuration
Apple		http://lists.apple.com/archives/security-announce/2007/Apr/msg00000.html	
CVE-2007-0734, CVE-2007-1338			

ASTERISK

Déni de service de 'Asterisk'			
Une erreur de conception peut permettre de provoquer un déni de service de l'interface de gestion du produit.			
Moyenne	25/04	Asterisk	
Correctif existant		Authentification 'MD5'	Erreur de conception
Full Disclosure		http://lists.grok.org.uk/pipermail/full-disclosure/2007-April/053968.html	

CA

Exécution de code arbitraire dans BrightStor ArcServe			
De multiples débordements de buffer peuvent permettre à un attaquant distant d'exécuter du code arbitraire.			
Forte	25/04	Se référer à l'avis orignal	
Correctif existant		Service 'SUN' 'RPC'	Débordement de buffer
CA		http://supportconnectw.ca.com/public/storage/infodocs/babmedser-secnotice.asp	
CVE-2007-2139			

CANON

"Cross-Site Scripting" dans Canon Network Camera Server

Un manque de validation permet à un attaquant distant de mener des attaques "CSS" contre des utilisateurs.

Forte	19/04	Canon 'Network Camera Server VB100 Series'	
Correctif existant		Non disponible	Validation insuffisante des données
Canon		http://secunia.com/advisories/24940/	

CISCO

Déni de service de plusieurs produits Cisco

De multiples failles peuvent entraîner des dénis de service.

Forte	29/03	Cisco 'Cisco Unified CallManager' version 3.3, 4.1, 4.2, 5.0 et ' Cisco Unified Presence Server' version 1.0	
Correctif existant		Protocoles SCCP,SCCPS,ICMP, ...	Non disponible
Cisco		http://www.cisco.com/warp/public/707/cisco-sa-20070328-voip.shtml	

Erreur de conception de 'NetFlow Collection Engine'

Une erreur de conception peut permettre à un attaquant distant d'obtenir un accès avec des privilèges élevés.

Forte	26/04	Cisco 'NetFlow Collection Engine' version 6.0 et inférieures	
Correctif existant		Gestion des comptes utilisateurs	Erreur de conception
Cisco		http://www.cisco.com/warp/public/707/cisco-sa-20070425-nfc.shtml	

Multiples failles dans 'Wireless Control System'

Plusieurs failles peuvent entraîner entre autres choses, des dénis de service et l'exposition d'informations.

Forte	12/04	Cisco 'Wireless Control System' versions inférieures à 4.0.96.0	
Correctif existant		Sauvegarde via 'FTP'	Erreur de conception
Cisco		http://www.cisco.com/warp/public/707/cisco-sa-20070412-wcs.shtml	

Multiples failles dans 'Wireless LAN Controller'

De multiples failles peuvent entraîner de multiples dommages, dont des dénis de service et l'exposition d'informations.

Forte	12/04	Cisco 'Wireless LAN Controller' version 4.0, version 3.2 et inférieures	
Correctif existant		Divers	Erreurs de conception et de configuration
Cisco		http://www.cisco.com/warp/public/707/cisco-sa-20070412-wlc.shtml	

CLAMAV

Multiples failles dans 'ClamAV'

L'anti-virus 'ClamAV' est vulnérable à plusieurs failles qui peuvent entraîner l'exposition d'informations.

Moyenne	13/04	ClamAV 'ClamAV' versions inférieures à 0.90.2	
Correctif existant		Divers	Débordement de buffer
ClamAV		http://sourceforge.net/project/shownotes.php?release_id=500765	
CVE-2007-1745, CVE-2007-1997			

COSIGN

Contournement de l'authentification de 'cosign'

Deux failles autorisent un attaquant distant à contourner l'authentification du produit.

Forte	12/04	Cosign 'Cosign' version 2.0.2 et inférieures et versions inférieures à 1.9.4b	
Correctif existant		Démon 'cosign'	Validation insuffisante des données
Cosign		http://www.umich.edu/~umweb/software/cosign/cosign-vuln-2007-001.txt	
Cosign		http://www.umich.edu/~umweb/software/cosign/cosign-vuln-2007-002.txt	

FETCHMAIL

Vulnérabilité dans l'implémentation 'APOP'

Une faille permet à un attaquant distant de mener des attaques de type "man-in-the-middle".

Forte	06/04	Fetchmail 'fetchmail' versions inférieures à 6.3.8	
Correctif existant		Protocole 'POP3'	Erreur de conception
Fetchmail		http://fetchmail.berlios.de/fetchmail-SA-2007-01.txt	
CVE-2007-1558			

FILEZILLA

Failles dans le client FTP 'FileZilla'

De multiples failles, aux conséquences inconnues, affectent 'FileZilla'.

Moyenne	17/04	FileZilla 'FileZilla' versions inférieures à 2.2.32	
Correctif existant		Non disponible	Erreur de chaîne de formatage, Déréférencement de pointeur NULL
FileZilla		http://sourceforge.net/project/shownotes.php?release_id=501534&group_id=21558	

FREERADIUS

Déni de service dans 'FreeRADIUS'

Un manque de validation peut permettre à un attaquant de provoquer un déni de service de ce serveur.

Forte	13/04	FreeRADIUS 'FreeRADIUS' version 1.1.5 et inférieures	
Correctif existant		'EAP-TTLS' et 'DIAMETER'	Manque de validation
FreeRADIUS		http://www.freeradius.org/security.html	

HP

Accès non autorisé dans HP StorageWorks

Une faille non documentée peut permettre à un utilisateur local d'obtenir un accès non autorisé.

Forte	26/04	Se référer à l'avis original	
Correctif existant		Non disponible	Non disponible
HP (SSRT071330)		http://www4.itrc.hp.com/service/cki/docDisplay.do?docId=HPSBST02200	

Déni de service via 'sendmail' sur 'HP-UX'

Une faille non documentée dans 'HP-UX' avec 'sendmail' permet de provoquer un déni de service.

Moyenne	16/04	HP 'HP-UX' version B.11.00, B.11.11, B.11.23	
Correctif existant		'sendmail'	Non disponible
HP (SSRT061243)		http://www4.itrc.hp.com/service/cki/docDisplay.do?docId=c00841370	

Elévation de privilèges dans 'HP-UX'

Sous certaines conditions, une faille non documentée dans 'HP-UX' permet d'obtenir des droits privilégiés à distance.

Forte	04/04	HP 'HP-UX' version B.11.00, B.11.11, B.11.23	
Correctif existant		'Portable File System' ('PFS')	Non disponible
HP (SSRT071339)		http://www5.itrc.hp.com/service/cki/docDisplay.do?docId=c00913684	

Exécution de code via 'Power Manager Remote Agent'

Une faille non documentée peut permettre à un utilisateur local malveillant d'exécuter du code arbitraire.

Forte	27/04	HP 'HP-UX' version B.11.11et B.11.23, HP 'Power Manager Remote Agent'	
Correctif existant		'Power Manager Remote Agent'	Non disponible
HP (SSRT061285)		http://www4.itrc.hp.com/service/cki/docDisplay.do?docId=emr_na-c00819543-1	

Faille dans un ActiveX de 'Mercury Quality Center'

Une faille non documentée dans un contrôle ActiveX de 'Mercury Quality Center' permet d'exécuter du code arbitraire sur un poste client Windows vulnérable.

Forte	27/03	HP 'Mercury Quality Center' version 8.2 SP1, version 9.0	
Correctif existant		Contrôle ActiveX	Non disponible
HP (SSRT071312)		http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c00901872	

Déni de service dans 'HP-UX'

Une faille non documentée dans 'HP-UX' autorise un utilisateur local à provoquer un déni de service.

Moyenne	04/04	HP 'HP-UX' version B.11.00	
Correctif existant		'ARPA'	Non disponible
HP (SSRT061120)		http://www5.itrc.hp.com/service/cki/docDisplay.do?docId=c00944467	

IBM

"Cross-Site Scripting" dans 'Lotus Domino Web Access'

Une faille non documentée autorise un attaquant distant à mener des attaques de type "Cross-Site Scripting".

Forte	29/03	IBM 'Lotus Domino Web Access' version 6.5 et version 7.0	
Correctif existant		Messages 'MIME'	Non disponible
IBM		http://www-1.ibm.com/support/docview.wss?rs=477&uid=swg21247201	

Déni de service de 'WebSphere Application Server'

Deux failles permettent de provoquer un déni de service du produit et l'exposition d'informations.

Forte	05/04	IBM 'WebSphere Application Server' version 6.1.0.5 et inférieures	
Correctif existant		'Java Message Service' (JMS)	Non disponible
IBM		http://www-1.ibm.com/support/docview.wss?uid=swg27007951#6107	
CVE-2007-1944, CVE-2007-1945			

Elévation de privilèges via la commande 'drmgr'

Un débordement de buffer de la plate-forme IBM 'AIX' autorise un utilisateur local à élever ses privilèges.

Moyenne	29/03	IBM 'AIX' version 5.2 et 5.3	
Correctif existant		Commande 'drmgr'	Débordement de buffer
IBM		http://www-1.ibm.com/support/docview.wss?uid=isg1IY95054	
IBM		http://www-1.ibm.com/support/docview.wss?uid=isg1IY96753	
IBM		http://www-1.ibm.com/support/docview.wss?uid=isg1IY96772	

Exposition d'informations dans 'TBSM'			
Une faille autorise un utilisateur local à obtenir des mots de passe et à élever ainsi ses privilèges.			
Moyenne	03/04	IBM 'Tivoli Business Service Manager' version 4.1	
Correctif existant		Fichiers 'ncisetup.db' , 'msi.log'	Erreur de conception
IBM		http://www-1.ibm.com/support/docview.wss?uid=swg24015473	

IPIX

Exécution de code dans l'ActiveX 'iPIX Image Well'			
Des débordements de buffer dans 'iPIX Image Well' peuvent entraîner l'exécution de code arbitraire.			
Forte	09/04	iPIX 'iPIX Image Well'	
Palliatif proposé		Contrôle ActiveX	Débordements de buffer
US-CERT		http://www.kb.cert.org/vuls/id/958609	
CVE-2007-1687			

KASPERSKY LABS

Corruption et exposition d'informations			
Deux failles autorisent un attaquant distant à corrompre des fichiers et à obtenir des informations.			
Forte	04/04	Kaspersky Labs 'Kaspersky Anti-Virus' et Kaspersky Labs 'Kaspersky Internet Security' version 6.0	
Correctif existant		Contrôle ActiveX 'SysInfo'	Erreur de conception
Kaspersky		http://www.kaspersky.com/technews?id=203038694	

Multiples failles dans Kaspersky Anti-Virus			
De multiples failles peuvent permettre à un attaquant local ou distant d'exécuter du code arbitraire.			
Forte	04/04	'Anti-Virus for File Server' et 'Anti-Virus for Workstations' versions inférieures à 6.0.2.678	
Correctif existant		Moteur d'analyse	Erreur de conception, Débordement de tas
Kaspersky		http://www.kaspersky.com/technews?id=203038693	

LIGHTTPD

Dénis de service via le serveur Web 'lighttpd'			
Deux failles permettent de provoquer un déni de service du serveur et/ou de la machine.			
Forte	16/04	Lighttpd 'lighttpd' version 1.4.13 et inférieures	
Correctif existant		Fonction 'mtime()'	Erreur de codage
lighttpd		http://www.lighttpd.net/assets/2007/4/13/lighttpd_sa2007_01.txt	
lighttpd		http://www.lighttpd.net/assets/2007/4/13/lighttpd_sa2007_02.txt	
CVE-2007-1869, CVE-2007-1870			

LINUX

Déni de service du noyau Linux			
Un manque de validation dans le noyau Linux peut entraîner une exécution de code arbitraire.			
Forte	13/04	Linux 'Noyau 2.6' versions inférieures à 2.6.21-rc6	
Correctif existant		Fichier 'fib_Semantics.c'	Validation insuffisante des données
SecurityFocus		http://www.securityfocus.com/bid/23447	
Kernel.org		http://kernel.org/pub/linux/kernel/v2.6/testing/ChangeLog-2.6.21-rc6	

Déni de service du noyau Linux 2.6			
Un débordement de pile dans le noyau Linux version 2.6 peut entraîner un déni de service du système.			
Forte	27/04	Linux 'Noyau 2.6' versions inférieures à 2.6.20.8	
Correctif existant		Fichier 'fib_frontend.c'	Débordement de pile
SecurityFocus		http://www.securityfocus.com/bid/23677	
Kernel.org		http://www.kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.20.8	

Exposition d'informations dans le noyau Linux 2.4			
Plusieurs manques de validation peuvent entraîner une exposition d'informations sensibles.			
Forte	24/04	Linux 'Noyau 2.4' version 2.4.34.2 et inférieures	
Correctif existant		Fonctions	Validation insuffisante des données
SecurityFocus		http://www.securityfocus.com/bid/23594	
Kernel.org		http://www.kernel.org/pub/linux/kernel/v2.4/ChangeLog-2.4.34.3	
CVE-2007-1353			

MEDIAWIKI

"Cross-Site Scripting" dans 'MediaWiki'			
Une faille permet à un attaquant distant de mener des attaques de type "Cross-Site Scripting".			
Moyenne	16/04	MediaWiki 'MediaWiki' versions inférieures à 1.6.9, à 1.7.2, à 1.8.3	
Correctif existant		Script 'index.php', module 'AJAX'	Validation insufisante des données
MediaWiki		http://sourceforge.net/forum/forum.php?forum_id=652721	
CVE-2007-0177			

MICROSOFT

Exécution de code arbitraire via Microsoft 'Agent'

Une faille permet à un attaquant distant d'exécuter du code arbitraire avec les droits de l'utilisateur courant.

Critique	10/04	Windows 2000, Windows Server 2003, Windows XP	
Correctif existant		'Agent' Microsoft	Corruption de la mémoire
Microsoft		http://www.microsoft.com/technet/security/Bulletin/MS07-020.mspx	
CVE-2007-1205			

Exécution de code arbitraire via 'UPnP'

Une corruption de la mémoire permet à un attaquant distant d'exécuter du code sur une machine vulnérable.

Critique	11/04	Microsoft Windows XP	
Correctif existant		Composant 'UPnP'	Corruption de la mémoire
Microsoft		http://www.microsoft.com/france/technet/security/bulletin/ms07-019.mspx	
CVE-2007-1204			

Exécution de code dans 'Content Management Server'

Deux failles peuvent permettre à un attaquant distant d'exécuter du code arbitraire et de mener des attaques 'CSS'

Critique	11/04	Microsoft 'Content Management Server 2001' version SP1, 'Content Management Server 2002' version SP2	
Correctif existant		Gestion des requêtes 'HTTP'	Corruption de la mémoire, Non disponible
Microsoft		http://www.microsoft.com/france/technet/security/bulletin/ms07-018.mspx	
CVE-2007-0938, CVE-2007-0939			

Exécution de code via le service 'DNS'

Un débordement de pile autorise un attaquant distant à exécuter du code arbitraire.

Forte	12/04	Windows 2000, Windows Server 2003	
Palliatif proposé		Service 'DNS', interface 'RPC'	Débordement de pile
Microsoft		http://www.microsoft.com/technet/security/advisory/935964.mspx	
CVE-2007-1748			

Exécutions de code dans les plate-formes Windows

De multiples failles peuvent entraîner l'exécution de code arbitraire locale ou distante.

Forte	03/04	Vista, Windows 2000, Windows Server 2003, Windows XP	
Correctif existant		Se référer à l'avis original	Se référer à l'avis original
Microsoft		http://www.microsoft.com/technet/security/Bulletin/MS07-017.mspx	
CVE-2006-5586, CVE-2006-5758, CVE-2007-0038, CVE-2007-1211, CVE-2007-1212, CVE-2007-1213, CVE-2007-1215			

Multiples vulnérabilités dans le processus 'CSRSS'

Plusieurs failles peuvent entraîner l'exécution de code, un déni de service et autoriser une élévation de privilèges.

Critique	10/04	Vista, Windows 2000, Windows Server 2003, Windows XP	
Correctif existant		Processus 'CSRSS'	Erreur de conception
Microsoft		http://www.microsoft.com/technet/security/Bulletin/MS07-021.mspx	
CVE-2006-6696, CVE-2006-6797, CVE-2007-1209			

Vulnérabilité dans la gestion des curseurs animés

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

Critique	29/03	Microsoft Windows 2000 version SP4, Server 2003 version SP1, Vista, XP version SP2	
Palliatif proposé		Gestion des curseurs animés	Erreur de codage
Microsoft		http://www.microsoft.com/technet/security/advisory/935423.mspx	

Elévation de privilèges dans le noyau Windows

Une faille permet à un utilisateur local d'élever ses privilèges.

Forte	10/04	Windows 2000 version SP4, Server 2003 version SP2 et inférieures, XP version SP2	
Correctif existant		Segments de mémoire mappés	Erreur de codage
Microsoft		http://www.microsoft.com/technet/security/Bulletin/MS07-022.mspx	
CVE-2007-1206			

MIT

Multiples vulnérabilités dans 'Kerberos 5'

Trois failles dans 'Kerberos 5' autorisent un attaquant distant à exécuter du code et à obtenir un accès non autorisé.

Critique	03/04	MIT 'Kerberos 5' version 1.6 et inférieures	
Correctif existant		Se référer à l'avis original	Se référer à l'avis original
MIT		http://web.mit.edu/kerberos/advisories/MITKRB5-SA-2007-001-telnetd.txt	
MIT		http://web.mit.edu/kerberos/advisories/MITKRB5-SA-2007-002-syslog.txt	
MIT		http://web.mit.edu/kerberos/advisories/MITKRB5-SA-2007-003.txt	
CVE-2007-0956, CVE-2007-0957, CVE-2007-1216			

NETBSD

Déni de service des plate-formes 'NetBSD'

Un manque de validation dans la commande 'iso' peut permettre à un utilisateur de provoquer un déni de service.

Forte	30/03	NetBSD 'NetBSD' version 2, version 3, version 4	
Correctif existant		Commande 'iso'	Validation insuffisante des données
NetBSD		ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2007-004.txt.asc	
CVE-2007-1677			

NOVELL

Déni de service de 'eDirectory'

Une faille non documentée peut permettre à un attaquant distant de provoquer un déni de service d'une machine.

Forte	27/04	Novell 'eDirectory' version 8.8.1, 8.8, 8.7.3.8 et inférieures	
Correctif existant		Gestion du protocole 'NCP'	Non disponible
Novell		http://www.novell.com/support/search.do?cmd=displayKC &externalId=3924657&sliceId=SAL_Public	
CVE-2006-4520			

Multiples failles dans Novell 'SecureLogin'

Plusieurs failles autorisent, entre autres choses, une élévation de privilèges.

Moyenne	06/04	Novell 'SecureLogin' version 6.0, version 6.0.1	
Correctif existant		Utilitaire 'ADSCHEMA'	Non disponible
Novell		http://download.novell.com/Download?buildid=NCwwjAbsgQQ~	

OPENAFS

Déni de service via 'OpenAFS' pour Windows

Une faille dans 'OpenAFS' pour Windows peut provoquer un déni de service d'un système vulnérable.

Forte	20/04	OPENAFS 'OpenAFS' version 1.5.18 et inférieures	
Correctif existant		Bibliothèque 'afslogon.dll'	Erreur de codage
OpenAFS		http://www.openafs.org/pages/security/OPENAFS-SA-2007-002.txt	

ORACLE

Nombreuses vulnérabilités dans les produits Oracle

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

Critique	17/04	Se référer à l'avis original	
Correctif existant		Se référer à l'avis original	Multiples vulnérabilités
Oracle		http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuapr2007.html	

PHPMYADMIN

"Cross-Site Scripting" dans 'phpMyAdmin'

Une erreur de conception peut permettre à un attaquant de mener des attaques de type "Cross-Site Scripting".

Forte	25/04	phpMyAdmin 'phpMyAdmin' version 2.10.0.2 et inférieures	
Correctif existant		Détection de code 'Javascript'	Erreur de conception
phpMyAdmin		http://www.phpmyadmin.net/home_page/security.php?issue=PMASA-2007-4	

POSTGRESQL

Elévation de privilèges dans 'PostgreSQL'

Une faille non documentée peut permettre à un utilisateur malveillant d'obtenir des privilèges élevés.

Forte	24/04	PostgreSQL 'PostgreSQL' version 7.x, 8.x	
Correctif existant		Fonctions 'SECURITY DEFINER'	Non disponible
PostgreSQL		http://www.postgresql.org/about/news.791	
CVE-2007-2138			

PROFTPD

Contournement de la sécurité dans 'ProFTPD'

Sous certaines conditions, une faille dans 'ProFTPD' permet de contourner certains mécanismes de sécurité.

Forte	19/04	ProFTPd 'ProFTPD' version 1.3 et inférieures, version 1.2.10 et inférieures	
Correctif existant		Composant 'Auth API'	Erreur de conception
ProFTPD Bugzilla		http://bugs.proftpd.org/show_bug.cgi?id=2922	

QUAGGA

Déni de service dans 'Quagga'

Une faille dans l'outil 'Quagga' permet de provoquer un déni de service.

Forte	11/04	Quagga 'Quagga' version 0.99.5	
Correctif existant		Démon 'bgpd'	Erreur de codage
Quagga		http://www.quagga.net/news2.php?y=2007&m=4&d=8#id1176073740	
Quagga Bugzilla		http://bugzilla.quagga.net/show_bug.cgi?id=354	

SNORT

Multiples failles dans 'Snort'

De multiples failles, aux conséquences inconnues, affectent l'outil de sécurité 'Snort'.

N/A	05/04	Snort 'Snort' versions inférieures à 2.6.1.4	
Correctif existant		Non disponible	Multiples problèmes
Snort		http://snort.org/docs/release_notes/release_notes_2614.txt	

SSH.COM

Elévation de privilèges via SSH Tectia Server

Un problème autorise des utilisateurs locaux à élever leurs privilèges.

Moyenne	12/04	SSH.COM 'SSH Tectia Server for IBM z/OS' versions inférieures à 5.4.0	
Correctif existant		Permissions sur les répertoires	Erreur de configuration
SSH.COM		http://www.ssh.com/documents/33/SSH_Tectia_Server_5.4.0_zOS_releasenotes.txt	

SUN

Déni de service dans 'Sun Cluster'

Une faille peut permettre à un utilisateur local de provoquer un déni de service d'une machine vulnérable.

Forte	25/04	Sun 'Sun Cluster ' version 3.1, version 3.2	
Correctif existant		Non disponible	Corruption de la mémoire
Sun		http://sunsolve.sun.com/search/document.do?assetkey=1-26-102874-1	

Denis de service dans 'Solaris'

Une faille autorise un attaquant distant à provoquer un déni de service d'une plate-forme vulnérable.

Forte	12/04	Sun 'Solaris' version 8, version 9	
Correctif existant		Implémentation 'IP'	Non disponible
Sun		http://sunsolve.sun.com/search/document.do?assetkey=1-26-102866-1	

Multiples failles dans 'Sun Java Web Console'

Une erreur de chaîne de formatage permet à un attaquant de provoquer un déni de service ou l'exécution de code.

Forte	17/04	Sun 'Sun Java Web Console' versions 2.2.2 à 2.2.5	
Correctif existant		Journalisation	Erreur de chaîne de formatage
Sun		http://sunsolve.sun.com/search/document.do?assetkey=1-26-102854-1	
CVE-2007-1681			

SYMANTEC

Exécution de code arbitraire dans 'ESM'

Un manque de validation autorise un attaquant à exécuter du code avec des droits privilégiés sur un système.

Forte	05/04	Symantec 'Enterprise Security Manager' toute versions	
Correctif existant		Interface de mise à jour	Erreur de conception
Symantec		http://www.symantec.com/avcenter/security/Content/2007.04.05d.html	

Multiples failles des produits Symantec

Deux failles peuvent entraîner une exposition d'informations sensibles et l'exécution de code arbitraire.

Forte	27/04	Se référer à l'avis original	
Correctif existant		Mécanisme de sauvegarde	Erreur de conception, Débordement de buffer
Symantec		http://www.symantec.com/avcenter/security/Content/2007.04.26.html	

TROLLTECH

Manque de validation dans la bibliothèque 'Qt'

Un manque de validation, aux conséquences inconnues, affecte la bibliothèque 'Qt'.

N/A	03/04	Trolltech 'Qt' version 3.3.8, 4.2.3	
Correctif existant		Caractères 'UTF-8'	Validation insuffisante des données
Trolltech		http://www.trolltech.com/company/newsroom/announcements/press.2007-03-30.9172215350	
CVE-2007-0242			

UNIX

Exécution de code arbitraire via 'man'

Une faille non documentée peut permettre à un utilisateur local malveillant d'exécuter du code arbitraire.

Moyenne	10/04	Unix 'man'	
Aucun correctif		Non disponible	Débordement de buffer
Debian		http://www.debian.org/security/2007/dsa-1278	
CVE-2006-4250			

X WINDOW

Multiple failles dans les serveurs 'X Window'			
De multiples failles peuvent permettre à un attaquant d'exécuter du code arbitraire avec des privilèges élevés.			
Forte	04/04	XFree86 'XFree86', X.Org 'X.Org' version 7.1-1.1.0, version X11R7.1	
Correctif existant		Se référer aux avis originaux	Se référer aux avis originaux
X.Org		http://lists.freedesktop.org/archives/xorg-announce/2007-april/0286.html	
Red Hat Bugzilla		https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=231684	
CVE-2007-1003, CVE-2007-1351, CVE-2007-1352, CVE-2007-1667			

YAHOO!

Exécution de code arbitraire dans 'Yahoo! Messenger'			
Un débordement de buffer peut permettre d'exécuter du code avec les privilèges de l'utilisateur courant.			
Forte	04/04	Yahoo! 'Yahoo! Messenger' version 8.x	
Correctif existant		Contrôl ActiveX	Débordement de buffer
Yahoo!		http://messenger.yahoo.com/security_update.php?id=031207	
CVE-2007-1680			

ALERTES NON CONFIRMEES

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

ADVENTNET

Exposition d'informations dans Firewall Analyzer			
Une faille dans 'ManageEngine Firewall Analyzer' permet à un attaquant d'obtenir des informations arbitraires.			
Forte	30/03	AdventNet 'ManageEngine Firewall Analyzer' version 4	
Correctif existant		Non disponible	Non disponible
SecurityFocus		http://www.securityfocus.com/bid/23097	

AIRCRACK-NG

Exécution de code arbitraire dans 'aircrack-ng'			
Un débordement de buffer peut permettre à un attaquant distant d'exécuter du code arbitraire.			
Forte	25/04	Aircrack-ng 'aircrack-ng' version 0.7 et inférieures	
Correctif existant		Non disponible	Débordement de buffer
nop-art		http://www.nop-art.net/advisories/airodump-ng.txt	
CVE-2007-2057			

AOL/MIRABILIS

Transfert de fichiers arbitraires dans 'ICQ' et 'AIM'			
Une faille autorise un utilisateur malveillant à tranférer des fichiers arbitraires vers un autre utilisateur.			
Moyenne	09/04	AOL/MIRABILIS 'AIM' version 5.9 et inférieures et 'ICQ' version 5.1	
Correctif existant		Transfert de fichiers	Traversée de répertoire
iDefense		http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=508	

AOL/NULLSOFT

Déni de service de 'Winamp' via des fichiers 'PLS'			
Une faille non documentée dans le lecteur multimédia 'Winamp' permet de provoquer un déni de service du produit.			
Forte	25/04	AOL/Nullsoft 'Winamp' version 5.33 et inférieures	
Aucun correctif		Gestion des fichiers 'PLS'	Non disponible
SecurityFocus		http://www.securityfocus.com/bid/23627	

Déni de service de 'Winamp' via des fichiers 'WMV'			
Un débordement de buffer dans le lecteur multimédia 'Winamp' permet de provoquer un déni de service du produit.			
Moyenne	19/04	AOL/Nullsoft 'Winamp' version 5.3	
Aucun correctif		Gestion des fichiers 'WMV'	Débordement de buffer
Bugtraq		http://marc.info/?l=bugtraq&m=117700724329672&w=2	

Exécution de code arbitraire dans 'Winamp'			
Plusieurs vulnérabilités dans des bibliothèques de 'Winamp' permettent l'exécution de code arbitraire.			
Forte	10/04	AOL/Nullsoft 'Winamp' version 5.33	
Correctif existant		Bibliothèques diverses	Corruption de la mémoire
Piotr Bania		http://www.piotrbania.com/all/adv/nullsoft-winamp-it_module-in_mod-adv.txt	
Piotr Bania		http://www.piotrbania.com/all/adv/nullsoft-winamp-libsndfile-adv.txt	
Piotr Bania		http://www.piotrbania.com/all/adv/nullsoft-winamp-s3m_module-in_mod-adv.txt	

APACHE

Déni de service de 'mod_perl'

Une erreur de codage dans le module Apache 'mod_perl' permet à un attaquant de provoquer un déni de service.

Forte	30/03	Apache 'mod_perl' version 1.x et version 2.x	
Correctif existant		Module mod_perl	Erreur de codage
Secunia		http://secunia.com/advisories/24678/	
CVE-2007-1349			

Exécution de code dans Apache 'suexec'

Plusieurs vulnérabilités peuvent permettre à un utilisateur local d'exécuter du code arbitraire.

Moyenne	11/04	Apache 'Apache' version 2.2.3	
Aucun correctif		Application 'suexec'	Conflit d'accès aux ressources, erreur de conception
iDefense		http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=511	
CVE-2007-1741			

APPLE

Exécution de code arbitraire dans 'Quicktime'

Une faille non documentée peut permettre à un attaquant distant d'exécuter du code arbitraire sur une machine.

Forte	24/04	Apple 'Quicktime'	
Aucun correctif		Non disponible	Non disponible
Matasano		http://www.matasano.com/log/812	

Exécution de code arbitraire dans 'Quicktime'

Deux faillespeuvent entraîner des dénis de service et l'exécution de code arbitraire.

Forte	26/04	Apple 'Quicktime' version 7.1.5 et inférieures	
Aucun correctif		Fichiers '.mov' et '.mp4',	Débordement de tas et d'entier
Security-Protocols		http://security-protocols.com/sp-x45-advisory.php	
Security-Protocols		http://security-protocols.com/sp-x46-advisory.php	

BMC SOFTWARE

Exécution de code arbitraire dans BMC 'Patrol'

Une corruption de la mémoire autorise un attaquant à exécuter du code arbitraire sur une machine vulnérable.

Forte	18/04	BMC Software 'Patrol'	
Correctif existant		Processus 'bgs_sdservice.exe'	Corruption de la mémoire
Zero Day		http://www.zerodayinitiative.com/advisories/ZDI-07-019.html	
CVE-2007-2136			

Exécution de code dans 'Performance Manager'

Une erreur de conception dans BMC 'Performance Manager' autorise un attaquant à exécuter du code arbitraire.

Forte	18/04	BMC Software 'Performance Manager'	
Aucun correctif		Processus 'PatrolAgent.exe'	Erreur de conception
Zero Day		http://www.zerodayinitiative.com/advisories/ZDI-07-020.html	
CVE-2007-1972			

CA

Exécution de code dans 'Brightstor ARCserve Backup'

Un débordement de buffer autorise un attaquant distant à exécuter du code arbitraire avec des droits privilégiés.

Critique	30/03	CA 'BrightStor ARCServe Backup' version r11.5 SP2 et inférieures	
Aucun correctif		Processus 'Mediasvr.exe'	Débordement de buffer
SecurityFocus		http://www.securityfocus.com/bid/23209	
Shirkdog		http://www.shirkdog.us/shk-004.html	

Injection de code SQL arbitraire dans CleverPath

Une erreur de conception peut permettre à un attaquant distant d'injecter du code SQL arbitraire.

Forte	25/04	CA 'CleverPath Portal'	
Correctif existant		Moteur de recherche	Erreur de conception
Hacktics		http://www.hacktics.com/AdvCleverPathApr07.html	

CHECK POINT

Elévation de privilèges dans 'ZoneAlarm'

Plusieurs manques de validation peuvent permettre à un utilisateur local d'élever ses privilèges et d'exécuter du code.

Forte	23/04	Check Point 'ZoneAlarm' version 5.0.156.0	
Correctif existant		Pilote 'srescan.sys'	Multiples manques de validation
iDefense		http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=517	

Déni de service via 'ZoneAlarm'			
Un manque de validation permet à un utilisateur local de provoquer un déni de service du système.			
Moyenne	15/04	Check Point 'ZoneAlarm Pro' version 6.1.744.001 et 6.5.737.000	
Correctif existant		Pilote 'vsdatant.sys'	Validation insuffisante des données
Matousec		http://www.matousec.com/info/advisories/ZoneAlarm-Multiple-insufficient-argument-validation-of-hooked-SSDT-functions.php	

CLAMAV

Déni de service dans 'ClamAV'			
Une faille dans l'antivirus 'ClamAV' peut permettre à un attaquant distant de provoquer un déni de service.			
Forte	26/04	ClamAV 'ClamAV'	
Aucun correctif		Traitement des fichiers 'PDF'	Non disponible
SecurityFocus		http://www.securityfocus.com/bid/23656	
CVE-2007-2029			

CLAROLINE

Injection de fichiers arbitraires dans 'Claroline'			
Un manque de validation peut permettre à un attaquant distant d'injecter des fichiers arbitraires.			
Moyenne	24/04	Claroline 'Claroline' version 1.8 rc1 et inférieures	
Aucun correctif		Paramètre 'rootSys'	Validation insuffisante des données
SecurityFocus		http://www.securityfocus.com/bid/23609	

COREL

Exécution de code arbitraire dans 'Wordperfect X3'			
Un débordement de pile dans 'Wordperfect X3' peut permettre à un attaquant distant d'exécuter du code arbitraire.			
Forte	29/03	Corel 'Wordperfect X3' version 13.0.0.565	
Aucun correctif		Traitement des fichiers '.PRS'	Validation insuffisante des données
Bugtraq		http://marc.info/?l=bugtraq&m=117509869120261&w=2	

Exécution de code dans 'Paint Shop Pro Photo'			
Un débordement de buffer non documenté peut permettre à un attaquant distant d'exécuter du code arbitraire.			
Forte	24/04	Corel 'Paint Shop Pro Photo' version 11.20	
Aucun correctif		Traitement des fichiers 'CLP'	Débordement de buffer
SecurityFocus		http://www.securityfocus.com/bid/23604	

DOTCLEAR

"Cross-Site Scripting" dans 'DotClear'			
Plusieurs manques de validation permettent à un attaquant distant de mener des attaques de type "CSS".			
Forte	11/04	DotClear 'DotClear' version 1.2.5 et inférieures	
Correctif existant		Scripts divers	Validation insuffisante des données
SecurityFocus		http://www.securityfocus.com/bid/23411	

DOVECOT

Exposition d'informations dans 'Dovecot'			
Une faille dans 'Dovecot' permet d'obtenir des informations.			
Moyenne	18/04	Dovecot 'Dovecot' versions inférieures à 1.0.rc29	
Correctif existant		Plugin 'zlib'	Erreur de conception
Dovecot-news		http://dovecot.org/pipermail/dovecot-news/2007-March/000039.html	

DPROXY

Exécution de code dans 'dproxy-nexgen'			
Un débordement de buffer dans 'dproxy-nexgen' autorise l'exécution de code arbitraire sur une machine vulnérable.			
Forte	02/04	DPROXY 'dproxy-nexgen'	
Aucun correctif		Fichier 'dns_decode.c'	Débordement de pile
Secunia		http://secunia.com/advisories/24688/	

EIQNETWORKS

Exécution de code dans 'Enterprise Security Analyzer'			
De multiples débordements peuvent entraîner l'exécution de code arbitraire.			
Forte	10/04	eIQnetworks 'Enterprise Security Analyzer' version 2.5 et inférieures	
Aucun correctif		Protocole 'ESA'	Débordement de tas, débordement d'entier
INfigo		http://www.infigo.hr/en/in_focus/advisories/INFIGO-2007-04-05	

ELINKS

Vulnérabilité dans 'elinks'

Une erreur de codage, aux conséquences inconnues, affecte le navigateur 'elinks'.

Moyenne	05/04	ELinks 'elinks' version 0.11	
Aucun correctif		Fichier 'loadmsgcat.c'	Erreur de codage, erreur de chaîne de formatage
Security.nnov		http://security.nnov.ru/news/Elinks/FS.html	
CVE-2007-2027			

ENTERASYS

Multiples failles dans les produits NetSight

Deux vulnérabilités autorisent un attaquant à provoquer un déni de service ou à exécuter du code arbitraire.

Forte	04/04	Enterasys 'NetSight Console' et 'NetSight Inventory Manager' version 2.1	
Correctif existant		Serveur 'TFTPD' et 'BOOTPD'	Débordement de buffer, Erreur de codage
iDefense		http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=506	

ETTERCAP

Déni de service de 'Ettercap-NG'

Une faille non documentée permet de provoquer un déni de service de 'Ettercap-NG'.

Forte	13/04	Ettercap 'Ettercap-NG' version 0.7.3	
Aucun correctif		Non disponible	Non disponible
SecurityFocus		http://www.securityfocus.com/bid/23474	

FOXIT

Déni de service de 'Foxit Reader'

Une faille non documentée peut entraîner un déni de service de l'application.

Moyenne	23/04	Foxit 'Foxit Reader' version 2.0	
Aucun correctif		Non disponible	Non disponible
SecurityFocus		http://www.securityfocus.com/bid/23576	

GIMP

Exécution de code arbitraire dans 'GIMP'

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

Forte	27/04	GIMP 'GIMP' version 2.2.14	
Aucun correctif		Module 'SUNRAS'	Débordement de buffer
SecurityFocus		http://www.securityfocus.com/bid/23680	

IBM

Failles dans 'Tivoli Provisioning Manager'

De multiples failles peuvent entraîner des dénis de service ou l'exécution de code avec des droits privilégiés.

Forte	02/04	IBM 'Tivoli Provisioning Manager for OS Deployment' version 5.1.0.116	
Correctif existant		POST 'multipart/form-data'	Multiples vulnérabilités
iDefense		http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=498	

"Cross-Site Scripting" dans 'Lotus Domino Web Access'

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

Forte	28/03	IBM 'Lotus Domino Web Access' version 7.0 et 6.5	
Correctif existant		Gestion des emails	Validation insuffisante des données
iDefense		http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=493	
CVE-2006-4843			

Déni de service et exécution de code dans Lotus Domino

Deux débordements peuvent provoquer un déni de service ou l'exécution de code arbitraire.

Forte	28/03	IBM 'Lotus Domino Server' version 6.5 et version 7.0	
Correctif existant		'nimap.exe' et composant LDAP	Débordements de buffer et de tas
iDefense		http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=494	
Zero Day		http://www.zerodayinitiative.com/advisories/ZDI-07-011.html	
CVE-2007-1675			

Exécution de code arbitraire via 'Lotus Sametime'

Un manque de validation permet à un attaquant d'exécuter du code arbitraire sur un poste vulnérable.

Forte	29/03	IBM 'Lotus Sametime' version 7.0 et version 6.5.1	
Correctif existant		Contrôle ActiveX	Validation insuffisante des données
iDefense		http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=495	

Exécution de code dans 'Tivoli Monitoring Express'			
Plusieurs services sont vulnérables à un débordement de tas qui peut entraîner l'exécution de code arbitraire.			
Forte	16/04	IBM 'Tivoli Monitoring Express' version 6.1	
Correctif existant		Se référer à l'avis original	Débordement de tas
Zero Day		http://www.zerodayinitiative.com/advisories/ZDI-07-018.html	
CVE-2007-2137			

IMAGEMAGICK

Exécution de code dans 'ImageMagick'			
Plusieurs débordements peuvent entraîner l'exécution de code dans les applications utilisant cette bibliothèque.			
Forte	31/03	ImageMagick 'ImageMagick' versions inférieures à 6.3.3-5	
Correctif existant		Images 'DCM' et 'XWD'	Débordement d'entier
iDefense		http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=496	

IPSEC-TOOLS

Déni de service de 'Ipsec-tools'			
Une faille non documentée dans l'outil 'Ipsec-tools' permet d'interrompre des tunnels existants.			
Forte	06/04	IPSEC-TOOLS 'Ipsec-tools' versions inférieures à 0.6.7	
Correctif existant		Fichier 'src/racoon/isakmp_inf.c'	Non disponible
Ipsec-tools		http://sourceforge.net/mailarchive/message.php?msg_name=20070406123739.GA1546%40zen.inc	
CVE-2007-1841			

IPSWITCH

Déni de service de 'WS_FTP Home 2007'			
Un déréférencement de pointeur NULL peut entraîner un déni de service de l'application.			
Moyenne	23/04	IpSwitch 'WS_FTP Home 2007'	
Aucun correctif		'NetscapeFTPHandler'	Déréférencement de pointeur NULL
Bugtraq		http://marc.info/?l=bugtraq&m=117718973730743&w=2	

K5N.US

"Cross-Site Scripting" via 'WebCalendar'			
Un manque de validation peut permettre à un attaquant de mener des attaques de types "Cross-Site Scripting".			
Forte	23/04	k5n.us 'WebCalendar' versions inférieures à 1.0.4	
Correctif existant		Script 'export_handler.php'	Validation insuffisante des données
Secunia		http://secunia.com/advisories/23341	

LANDESK

Exécution de code dans LANDesk 'Management Suite'			
Un débordement de pile autorise un attaquant à exécuter du code arbitraire avec des droits privilégiés.			
Forte	13/04	LANDESK 'Management Suite' version 8.7	
Correctif existant		Service 'Alert'	Débordement de pile
TippingPoint		http://www.tippingpoint.com/security/advisories/TSRT-07-04.html	
CVE-2007-1674			

LDAP ACCOUNT MANAGER

Injection de scripts HTML dans 'LAM'			
Une erreur de codage dans 'LAM' peut permettre à un attaquant distant d'injecter des scripts 'HTML' arbitraires.			
Forte	30/03	LDAP Account Manager 'LAM' version 1.2	
Correctif existant		Traitement des données 'LDAP'	Erreur de codage
SecurityFocus		http://www.securityfocus.com/bid/23190	

LINKSYS

Déni de service du produit Linksys 'SPA921'			
Une faille non documentée peut permettre à un attaquant distant de provoquer un déni de service.			
Forte	25/04	Linksys 'SPA941' version 5.1.5	
Correctif existant		Traitement des paquets 'SIP'	Non disponible
Full Disclosure		http://lists.grok.org.uk/pipermail/full-disclosure/2007-April/053959.html	

LINUX

Débordement de buffer du noyau Linux			
Un débordement de buffer peut permettre à un utilisateur local d'exécuter du code arbitraire.			
Forte	06/04	Linux 'Noyau 2.6' version 2.6.20 et inférieures	
Correctif existant		Bibliothèque 'libcapi'	Débordement de buffer
Security Focus		http://www.securityfocus.com/bid/23333	
CVE-2007-1217			

Dénis de service dans le noyau Linux			
Deux failles permettent de provoquer des dénis de service du noyau et d'exécuter du code arbitraire.			
Forte	11/04	Linux 'Noyau 2.6' versions inférieures à 2.6.20.5	
Correctif existant		Module 'AppleTalk'	Erreur de codage, Débordement de buffer
SecurityFocus		http://www.securityfocus.com/bid/23376	
SecurityFocus		http://www.securityfocus.com/bid/23384	

MADWIFI

Déni de service de 'MadWiFi' en mode 'Ad-Hoc'			
Une faille non documentée permet à un attaquant distant de provoquer un déni de service d'un système vulnérable.			
Forte	11/04	MADWiFi 'MadWiFi' versions inférieures à 0.9.3	
Correctif existant		Mode 'Ad-Hoc'	Non disponible
SecurityFocus		http://www.securityfocus.com/bid/23433	
CVE-2006-7177			

Déni de service et exposition d'informations			
De multiples failles peuvent entraîner des dénis de service de la plate-forme et entraîner l'exposition d'informations.			
Forte	03/04	MADWiFi 'MadWifi' versions inférieures à 0.9.3	
Correctif existant		Divers	Erreur de codage
Secunia		http://secunia.com/advisories/24670/	
CVE-2006-7178, CVE-2006-7179, CVE-2006-7180			

MCAFEE

Exécution de code dans 'VirusScan Enterprise'			
Un débordement de buffer autorise un attaquant à provoquer un déni de service du produit ou l'exécution de code.			
Forte	17/04	McAfee 'VirusScan Enterprise' version 8.0i Patch 11 et inférieures	
Correctif existant		Composant 'On-Access scanner'	Débordement de buffer
iDefense		http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=515	

Déni de service de 'e-Business Server'			
Une vulnérabilité autorise un attaquant à provoquer un déni de service d'un composant de ce produit.			
Forte	17/04	McAfee 'e-Business Server' version 8.5.1 et inférieures, version 8.1.0 et inférieures	
Correctif existant		Serveur d'administration	Erreur de codage
iDefense		http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=516	

MICROSOFT

Multiples failles 'IPv6' dans 'Windows Vista'			
De multiples failles peut permettre de provoquer des dénis de service et d'usurper un certain nombre de services.			
Critique	30/03	Vista	
Aucun correctif		Composant 'LLTD'	Multiples failles
Securityvulns		http://securityvulns.com/news/Microsoft/Vista/IPv6/MB.html	
Symantec		http://www.symantec.com/avcenter/reference/Vista_Network_Attack_Surface_RTM.pdf	
CVE-2007-1527, CVE-2007-1528, CVE-2007-1529, CVE-2007-1530, CVE-2007-1531, CVE-2007-1532, CVE-2007-1533, CVE-2007-1534, CVE-2007-1535			

Déni de service de 'Windows Vista'			
Une faille peut entraîner un déni de service du système.			
Forte	30/03	Microsoft Windows Vista	
Aucun correctif		Pilote 'atikmdag.sys'	Non disponible
Secunia		http://secunia.com/advisories/24667/	

Déni de service de 'Windows XP'			
Une faille non documentée dans les plate-formes 'Windows XP' peut entraîner un déni de service.			
Moyenne	06/04	Microsoft Windows XP	
Aucun correctif		Traitement des images 'BMP'	Non disponible
IVAN FRATRIC		http://ifsec.blogspot.com/2007/04/several-windows-image-viewers.html	

Déni de service du navigateur 'Internet Explorer'			
Une faille provoque un déni de service du produit à l'aide d'une page HTML.			
Forte	28/03	Microsoft 'Internet Explorer' version 7.0	
Aucun correctif		Non disponible	Non disponible
SecurityFocus		http://www.securityfocus.com/bid/23178	

Exécution de code dans 'Word 2007'			
Un débordement de bufferpermet d'exécuter du code arbitraire avec les droits de l'utilisateur courant.			
Forte	09/04	Microsoft 'Word 2007'	
Aucun correctif		Bibliothèque 'wwlib.dll'	Débordement de buffer
SecurityFocus		http://www.securityfocus.com/bid/23380	

Exécution de code via la visionneuse d'aide			
Une faille dans la visionneuse d'aide des plate-formes Windows permet d'exécuter du code arbitraire.			
Forte	10/04	Microsoft Windows 2000, Server 2003, XP	
Aucun correctif		Visionneuse d'aide	Débordement de tas
SecurityFocus		http://www.securityfocus.com/bid/23382	

MYDNS

Débordement de tas dans 'MyDNS'			
Un débordement de tas, aux conséquences inconnues, affecte le serveur DNS 'MyDNS' pour plate-formes UNIX.			
Forte	27/04	MyDNS 'MyDNS' version 1.10	
Correctif existant		Fichier 'update.c'	Débordement de tas
Full Disclosure		http://lists.grok.org.uk/pipermail/full-disclosure/2007-April/054024.html	

NAVIGATEURS

"HTTP Request Splitting" dans plusieurs navigateurs Web			
Une faille peut permettre à un attaquant distant de mener des attaques de type "HTTP Request Splitting".			
Forte	27/04	Microsoft 'Internet Explorer' version 7.0.5730.11 et inférieures, Mozilla 'Firefox' version 2.0.0.3 et inférieures	
Aucun correctif		Valeur 'HTTP Digest	Non disponible
SecurityTracker		http://www.securitytracker.com/alerts/2007/Apr/1017968.html	
SecurityTracker		http://www.securitytracker.com/alerts/2007/Apr/1017969.html	
Wisec		http://www.wisec.it/vulns.php?id=11	

NORTEL

Multiples vulnérabilités dans Nortel 'VPN Router'			
De multiples failles permettent d'obtenir un accès non autorisé et de corrompre un équipement vulnérable.			
Forte	18/04	Nortel 'VPN Router'	
Correctif existant		Comptes utilisateurs	Erreur de configuration
Nortel		http://www130.nortelnetworks.com/go/main.jsp?cscat=BLTNDETAIL&DocumentOID=567877&poid=null	

NOVELL

Exécution de code arbitraire dans 'Groupwise WebAccess'			
Un débordement de pile autorise un attaquant distant à exécuter du code arbitraire.			
Forte	19/04	Novell 'Groupwise WebAccess' versions inférieures à 7.0 SP2	
Correctif existant		Processus 'GWINTER.exe'	Débordement de pile
Zero Day		http://www.zerodayinitiative.com/advisories/ZDI-07-015.html	
CVE-2007-2171			

ORACLE

Exposition d'informations dans 'Oracle Applications'			
Une faille peut permettre à un attaquant distant d'obtenir, sous certaines conditions, des informations sensibles.			
Forte	13/04	Oracle 'Oracle Applications' version 11i	
Aucun correctif		Non disponible	Erreur de conception
SecurityFocus		http://www.securityfocus.com/bid/23446	
Integrigy		http://www.integrigy.com/security-resources/advisories/Integrigy_Encrypted_Password_Disclosure.pdf	

PHP

Exécution de code dans 'PHP'			
De multiples failles permettent de provoquer l'exposition d'informations, des dénis de service et l'exécution de code.			
Forte	30/04	PHP 'PHP' versions inférieures à 4.4.5, 5.2.1	
Aucun correctif		Se référer à l'avis original	Se référer à l'avis original
MoPB		http://www.php-security.org/MOPB/MOPB-38-2007.html MOPB-39-2007.html MOPB-40-2007.html	
MoPB		http://www.php-security.org/MOPB/MOPB-41-2007.html MOPB-42-2007.html MOPB-43-2007.html	
MoPB		http://www.php-security.org/MOPB/MOPB-44-2007.html	

Exposition d'informations via la fonction 'iptcembed()'			
Une erreur de conception autorise un attaquant à obtenir des informations arbitraires.			
Moyenne	29/03	PHP 'PHP' version 4.4.6 et inférieures, 5.2.1 et inférieures	
Aucun correctif		Gestionnaire d'erreurs	Erreur de conception
MoPB		http://www.php-security.org/MOPB/MOPB-37-2007.html	

Injection et exécution de code arbitraire dans 'PHP			
Deux failles permettent d'injecter du code arbitraire, de provoquer un déni de service ou d'exécuter du code.			
Forte	10/04	PHP 'PHP' version 5.2.0, 5.2.1	
Aucun correctif		'FILTER_VALIDATE_EMAIL',	Erreur de conception, Débordement d'entier
PMOPB		http://www.php-security.org/MOPB/PMOPB-45-2007.html	
CVE-2007-1001			

Contournement de la restriction 'open_basedir'			
Une erreur de conception dans 'PHP' permet de contourner la restriction de sécurité 'open_basedir'.			
Moyenne	28/03	PHP 'PHP' versions inférieures à 4.4.5, à 5.2.1	
Correctif existant		Restriction de sécurité	Erreur de conception
MoPB		http://www.php-security.org/MOPB/MOPB-36-2007.html	

PYTHON

Exposition d'informations via 'Python'			
Une erreur de codage dans une fonction de 'Python' autorise un utilisateur local à obtenir des informations.			
Moyenne	31/03	Python 'Python' version 2.4, 2.5	
Aucun correctif		'Modules/_localemodule.c'	Erreur de codage
Debian Bug report		http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=416934	
CVE-2007-2052			

SAP

Multiples vulnérabilités dans 'SAP'			
De multiples failles peuvent permettre à un attaquant d'obtenir des informations sensibles, de provoquer des dénis de service et d'exécuter du code.			
Forte	05/04	SAP 'SAP RFC Library' version 6.40, version 7.00	
Correctif existant		Se référer à l'avis original	Se référer à l'avis original
CYBSEC		CYBSEC-Security_Advisory_SAP_RFC_SET_REG_SERVER_PROPERTY_RFC_Function_Denial_of_Service.pdf	
CYBSEC		CYBSEC-Security_Advisory_SAP_RFC_START_GUI_RFC_Function_Buffer_Overflow.pdf	
CYBSEC		CYBSEC-Security_Advisory_SAP_RFC_START_PROGRAM_RFC_Function_Multiple_Vulnerabilities.pdf	
CYBSEC		CYBSEC-Security_Advisory_SAP_SYSTEM_CREATE_INSTANCE_RFC_Function_Buffer_Overflow.pdf	
CYBSEC		CYBSEC-Security_Advisory_SAP_TRUSTED_SYSTEM_SECURITY_RFC_Function_Information_Disclosure.pdf	

SECURE COMPUTING

"Cross-Site Scripting" dans 'IronMail'			
L'interface d'administration est vulnérable à des attaques de type "Cross-Site Scripting".			
Forte	28/03	Secure Computing 'IronMail' version 6.1.1	
Aucun correctif		Console d'administration	Validation insuffisante des données
SecurityTracker		http://securitytracker.com/id?1017821	
CVE-2007-1723			

SYMANTEC

Exécution de code dans 'Norton Personal Firewall 2006'			
Des manques de validation peuvent permettre à un utilisateur d'exécuter du code avec des privilèges élevés.			
Forte	03/04	Symantec 'Norton Personal Firewall 2006' version 9.1.1.7, version 9.1.0.33	
Aucun correctif		Composant 'SSDT'	Validation insuffisante des données
Matousec		http://www.matousec.com/info/advisories/Norton-Multiple-insufficient-argument-validation-of-hooked-SSDT-functions.php	

TRUECRYPT

Elévation de privilèges et exposition d'informations			
Une erreur de conception peut être exploitée afin d'obtenir des droits privilégiés ou des informations.			
Moyenne	28/03	TrueCrypt 'TrueCrypt' version 4.3 et inférieures	
Aucun correctif		Mode 'set-uid root' activé	Erreur de conception
Bugtraq		http://www.securityfocus.com/archive/1/464064	

UNIX

Déni de service via 'file'			
Une faille non documentée dans l'utilitaire 'file' autorise un utilisateur à provoquer un déni de service d'un système.			
Forte	18/04	Unix 'file' version 4.20	
Aucun correctif		Rxpressions régulières	Non disponible
Security.nnov		http://security.nnov.ru/news/FILE/regexp/DoS.html	
CVE-2007-2026			

VIXIE CRON

Déni de service de 'Vixie Cron'			
Une faille dans 'Vixie Cron' permet à un utilisateur local d'empêcher l'exécution de fichiers 'cron'.			
Moyenne	16/04	Vixie cron 'Vixie Cron' version 4.1, 3.0.1	
Aucun correctif		Gestion des liens	Erreur de conception
SecurityFocus		http://www.securityfocus.com/bid/23520	
CVE-2007-1856			

VMWARE

Multiples failles dans 'ESX Server'

Deux failles peuvent permettre à un attaquant de provoquer un déni de service et d'exécuter du code.

Forte	05/04	VMWare 'ESX Server' version 3.0.0, version 3.0.1	
Correctif existant		Non disponible	Double libération de mémoire, Débordement de buffer
Full Disclosure		http://lists.grok.org.uk/pipermail/full-disclosure/2007-April/053483.html	

CVE-2007-1270, CVE-2007-1271

WORDPRESS

Injection de code SQL arbitraire via 'WordPress'

Une failleautorise un attaquant distant à injecter du code arbitraire dans la base de données sous-jacente.

Forte	03/04	WordPress 'WordPress' version 2.1.2	
Aucun correctif		Non disponible	Validation insuffisante des données
SecurityFocus		http://www.securityfocus.com/bid/23294	

Elévation de privilèges dans 'WordPress'

Une faille dans 'WordPress' autorise un utilisateur à obtenir des droits privilégiés afin de publier des notes.

Moyenne	06/04	WordPress 'WordPress' version 2.1.2	
Correctif existant		Script 'xmlrpc.php'	Erreur de conception
Full Disclosure		http://lists.grok.org.uk/pipermail/full-disclosure/2007-April/053564.html	

XMMS

Exécution de code arbitraire dans 'XMMS'

Deux débordements d'entierpeuvent permettre à un attaquant distant d'exécuter du code arbitraire.

Moyenne	21/03	XMMS 'XMMS' version 1.2.10	
Aucun correctif		Habillages graphiques ('skin')	Débordement d'entier
Secunia		http://secunia.com/secunia_research/2007-47/advisory/	

CVE-2007-0653, CVE-2007-0654

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:

CIAC

Reprise de l'avis Apple APPLE-SA-2007-04-19

Le CIAC a repris, sous la référence R-216, l'avis Apple APPLE-SA-2007-04-19 concernant de nombreuses vulnérabilités dans 'Mac OS X' et 'Mac OS X Server' qui peuvent entraîner de multiples conséquences, dont des dénis de service d'applications et l'exécution de code arbitraire.

http://www.ciac.org/ciac/bulletins/r-216.shtml

CVE-2006-0300, CVE-2006-5867, CVE-2006-6143, CVE-2006-6652, CVE-2007-0022, CVE-2007-0465, CVE-2007-0646, CVE-2007-0724, CVE-2007-0725, CVE-2007-0729, CVE-2007-0732, CVE-2007-0734, CVE-2007-0735, CVE-2007-0736, CVE-2007-0737, CVE-2007-0738, CVE-2007-0739, CVE-2007-0741, CVE-2007-0742, CVE-2007-0743, CVE-2007-0744, CVE-2007-0746, CVE-2007-0747, CVE-2007-0957, CVE-2007-1216

Reprise de l'avis CA 136549

Le CIAC a repris, sous la référence R-217, l'avis CA 136549 concernant de multiples débordements de buffer dans 'BrightStor ARCserve Backup' qui peuvent permettre à un attaquant distant d'exécuter du code arbitraire.

http://www.ciac.org/ciac/bulletins/r-217.shtml

CVE-2007-1785, CVE-2007-2139

Reprise de l'avis Cisco 82078

Le CIAC a repris, sous la référence R-218, l'avis Cisco 82078 concernant une erreur de conception dans 'NetFlow Collection Engine' qui peut permettre à un attaquant distant d'obtenir un accès au produit avec des privilèges élevés.

http://www.ciac.org/ciac/bulletins/r-218.shtml

Reprise de l'avis Cisco 82128

Le CIAC a repris, sous la référence R-207, l'avis Cisco 82128 concernant plusieurs failles dans Cisco 'Wireless Control System' qui peuvent entraîner entre autres choses, des dénis de service et l'exposition d'informations.

http://www.ciac.org/ciac/bulletins/r-207.shtml

Reprise de l'avis Cisco 82129

Le CIAC a repris, sous la référence R-206, l'avis Cisco 82129 concernant plusieurs failles dans le produit Cisco 'Wireless LAN Controller' qui peuvent entraîner de multiples dommages, dont des dénis de service et l'exposition d'informations.

http://www.ciac.org/ciac/bulletins/r-206.shtml

Reprise de l'avis Cisco 82327

Le CIAC a repris, sous la référence R-191, l'avis Cisco 82327 concernant de multiples failles dans les produits 'Cisco Unified CallManager' et 'Cisco Unified Presence Server' qui peuvent entraîner des dénis de service.

http://www.ciac.org/ciac/bulletins/r-191.shtml

Reprise de l'avis Debian DSA-1273

Le CIAC a repris, sous la référence R-190, l'avis Debian DSA-1273 discutant de multiples failles dans le paquetage 'nas' ('Network Audio System') sur Debian GNU/Linux version 3.1 (sarge) qui peuvent permettre à un attaquant distant de provoquer des dénis de service et d'obtenir des privilèges élevés.

http://www.ciac.org/ciac/bulletins/r-190.shtml

CVE-2007-1543, CVE-2007-1544, CVE-2007-1545, CVE-2007-1546, CVE-2007-1547

Reprise de l'avis Debian DSA-1277

Le CIAC a repris, sous la référence R-211, l'avis Debian DSA-1277 concernant deux débordements d'entier dans 'xmms' qui peuvent permettre à un attaquant distant d'exécuter du code arbitraire.

http://www.ciac.org/ciac/bulletins/r-211.shtml

CVE-2007-0653, CVE-2007-0654

Reprise de l'avis Debian DSA-1278

Le CIAC a repris, sous la référence R-210, l'avis Debian DSA-1278 concernant une faille non documentée dans la commande 'man' qui permet à un utilisateur local malveillant d'exécuter du code arbitraire.

http://www.ciac.org/ciac/bulletins/r-210.shtml

CVE-2006-4250

Reprise de l'avis HP HPSBGN02199

Le CIAC a repris, sous la référence R-205, l'avis HP HPSBGN02199 à propos d'une faille dans un contrôle ActiveX de 'Mercury Quality Center' qui permet d'exécuter du code arbitraire sur un poste client Windows vulnérable.

http://www.ciac.org/ciac/bulletins/r-205.shtml

Reprise de l'avis Intel INTEL-SA-00001

Le CIAC a repris, sous la référence R-197, l'avis Intel INTEL-SA-00001 concernant de multiples failles dans les pilotes WiFi Intel Centrino qui peuvent entraîner l'exécution de code arbitraire avec des droits privilégiés.

http://www.ciac.org/ciac/bulletins/r-197.shtml

Reprise de l'avis Microsoft

Le CIAC a repris, sous la référence R-199, l'avis Microsoft MS07-019 (931261) concernant une faille dans les plate-formes 'Windows XP' qui permet à un attaquant distant d'exécuter du code arbitraire sur une machine vulnérable.

http://www.ciac.org/ciac/bulletins/r-199.shtml

CVE-2007-1204

Reprise de l'avis Microsoft (925902) MS07-017

Le CIAC a repris, sous la référence R-192, l'avis Microsoft (925902) MS07-017 concernant de multiples failles dans Windows qui peuvent entraîner l'exécution de code arbitraire.

http://www.ciac.org/ciac/bulletins/r-192.shtml

CVE-2006-5586, CVE-2006-5758, CVE-2007-0038, CVE-2007-1211, CVE-2007-1212, CVE-2007-1213, CVE-2007-1215

Reprise de l'avis Microsoft 935964

Le CIAC a repris, sous la référence R-212, l'avis Microsoft 935964 concernant un débordement d'entier déclenché via l'interface 'RPC' du service 'DNS' des plate-formes Windows. Ceci peut entraîner l'exécution de code arbitraire.

http://www.ciac.org/ciac/bulletins/r-212.shtml

CVE-2007-1748

Reprise de l'avis Microsoft MS07-018

Le CIAC a repris, sous la référence R-198, l'avis Microsoft MS07-018 (925939) concernant deux failles dans le produit Microsoft 'CMS' qui permettent à un attaquant d'exécuter du code et de mener des attaques 'CSS'

http://www.ciac.org/ciac/bulletins/r-198.shtml

CVE-2007-0938, CVE-2007-0939

Reprise de l'avis Microsoft MS07-020

Le CIAC a repris, sous la référence R-200, l'avis Microsoft MS07-020 (932168) concernant une faille dans Microsoft 'Agent' qui permet à un attaquant distant d'exécuter du code arbitraire avec les droits de l'utilisateur courant.

http://www.ciac.org/ciac/bulletins/r-200.shtml

CVE-2007-1205

Reprise de l'avis Microsoft MS07-021

Le CIAC a repris, sous la référence R-201, l'avis Microsoft MS07-021 (930178) concernant plusieurs failles dans le processus 'CSRSS' qui peuvent entraîner l'exécution de code et autoriser un utilisateur à élever ses privilèges.

http://www.ciac.org/ciac/bulletins/r-201.shtml

CVE-2006-6696, CVE-2006-6797, CVE-2007-1209

Reprise de l'avis Microsoft MS07-022

Le CIAC a repris, sous la référence R-203, l'avis Microsoft MS07-022 (931784) concernant une faille dans le noyau des plate-formes Windows qui permet à un utilisateur local d'élever ses privilèges.

http://www.ciac.org/ciac/bulletins/r-203.shtml

CVE-2007-1206

Reprise de l'avis Oracle d'avril 2007

Le CIAC a repris, sous la référence R-213, l'avis Oracle d'avril 2007 concernant de nombreuses failles dans les produits Oracle qui peuvent entraîner de multiples dommages.

http://www.ciac.org/ciac/bulletins/r-213.shtml

Reprise de l'avis Red Hat RHSA-2007:0095

Le CIAC a repris, sous la référence R-193, l'avis Red Hat RHSA-2007:0095 concernant une faille dans le démon 'telnetd' de 'Kerberos 5' sur les plate-formes Red Hat. Cette faille autorise un attaquant distant à obtenir un accès non autorisé à un machine vulnérable.

http://www.ciac.org/ciac/bulletins/r-193.shtml

CVE-2007-0956

Reprise de l'avis Red Hat RHSA-2007:0125

Le CIAC a repris, sous la référence R-194, l'avis Red Hat RHSA-2007:0125 concernant de multiples failles dans le serveur 'XFree86' sur les plate-formes Red Hat. Ces failles peuvent entraîner l'exécution de code arbitraire ou provoquer un déni de service.

http://www.ciac.org/ciac/bulletins/r-194.shtml

CVE-2007-1003, CVE-2007-1351, CVE-2007-1352, CVE-2007-1667

Reprise de l'avis Red Hat RHSA-2007:0127

Le CIAC a repris, sous la référence R-195, l'avis Red Hat RHSA-2007:0127 concernant une faille dans le serveur 'X.org' sur les plate-formes Red Hat. Cette vulnérabilités peut entraîner un déni de service ou l'exécution de code arbitraire.

http://www.ciac.org/ciac/bulletins/r-195.shtml

CVE-2007-1003

Reprise de l'avis Red Hat RHSA-2007:0132

Le CIAC a repris, sous la référence R-196, l'avis Red Hat RHSA-2007:0132 concernant de multiples failles dans 'libXfont' sur les plate-formes Red Hat. Ces vulnérabilités autorisent un attaquant distant à exécuter du code arbitraire.

http://www.ciac.org/ciac/bulletins/r-196.shtml

CVE-2007-1351, CVE-2007-1352

Reprise de l'avis Red Hat RHSA-2007:0155

Le CIAC a repris, sous la référence R-214, l'avis Red Hat RHSA-2007:0155 concernant plusieurs vulnérabilités dans 'PHP' sur les plate-formes Red Hat Enterprise Linux qui peuvent notamment entraîner des dénis de service et l'exécution de code arbitraire.

http://www.ciac.org/ciac/bulletins/r-214.shtml

CVE-2007-0455, CVE-2007-1001, CVE-2007-1285, CVE-2007-1286, CVE-2007-1583, CVE-2007-1711, CVE-2007-1718

Reprise de l'avis Sun 102885

Le CIAC a repris, sous la référence R-215, l'avis Sun 102885 concernant la vulnérabilité du navigateur 'Mozilla' version 1.7 fourni avec 'Solaris' versions 8, 9 et 10, à la faille référencée CVE-2006-6497 qui permet d'exécuter du code arbitraire ou de provoquer un déni de service du produit.

http://www.ciac.org/ciac/bulletins/r-215.shtml

CVE-2006-6497

Reprise de l'avis Symantec SYM07-003

Le CIAC a repris, sous la référence R-202, l'avis Symantec SYM07-003 concernant une vulnérabilité dans le produit Symantec 'ESM' ('Enterprise Security Manager') qui autorise un attaquant à exécuter du code arbitraire avec des droits privilégiés sur un système vulnérable.

http://www.ciac.org/ciac/bulletins/r-202.shtml

Reprise de l'avis US-CERT VU#958609

Le CIAC a repris, sous la référence R-208, l'avis US-CERT VU#958609 concernant de multiples débordements de buffer dans le contrôle ActiveX 'iPIX Image Well' qui peuvent entraîner l'exécution de code arbitraire.

http://www.ciac.org/ciac/bulletins/r-208.shtml

CVE-2007-1687

Reprise de l'avis US-CERT VU#972686

Le CIAC a repris, sous la référence R-209, l'avis US-CERT VU#972686 concernant une faille dans la pile 'TCP/IP' de 'HP-UX' qui permet de provoquer un déni de service du système à distance sous certaines conditions.

http://www.ciac.org/ciac/bulletins/r-209.shtml

CVE-2005-1192

Reprise de l'avis Yahoo! 031207

Le CIAC a repris, sous la référence R-204, l'avis Yahoo! 031207 concernant un débordement de buffer dans un contrôle ActiveX de 'Yahoo! Messenger' qui peut permettre à un attaquant distant d'exécuter du code arbitraire avec les privilèges de l'utilisateur courant.

http://www.ciac.org/ciac/bulletins/r-204.shtml

CVE-2007-1680

CISCO

Correctifs pour plusieurs applications Web

Cisco a annoncé, dans le bulletin 82377, la disponibilité de correctifs pour les applications Web 'Network Analysis Modules' ('NAM'), 'CiscoWorks Wireless LAN Solution Engine' ('WLSE'), 'CiscoWorks Wireless LAN Solution Engine Express' ('WLSX'), 'Cisco Unified Application Environment', 'Hosting Solution Engine' et 'Hosting Solution Software'. Ils corrigent des débordements de buffer dans les fonctions 'htmlentities()' et 'htmlspecialchars()' de 'PHP' peuvent être exploités afin d'exécuter du code arbitraire.

http://www.cisco.com/warp/public/707/cisco-sr-20070425-http.shtml

CVE-2006-5465

Révision de l'alerte Cisco 81734

Cisco a révisé l'alerte 81734 concernant une faille non documentée dans les équipements fonctionnant avec 'IOS' ou 'IOS XR' qui peut entraîner un déni de service ou l'exécution de code arbitraire. Cette révision met à jour les informations concernant les versions 12.2BC et 12.1EO de Cisco 'IOS' ainsi que la section "Workarounds".

http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-ip-option.shtml

Révision du bulletin 50961

Cisco a révisé le bulletin 50961 concernant la vulnérabilité de certains équipements à une attaque par déni de service. Cette révision met à jour les informations concernant le produit 'CallManager'.

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

Révision du bulletin 82129

Cisco a révisé le bulletin 82129 concernant de multiples failles dans le produit Cisco 'Wireless LAN Controller' qui peuvent entraîner de multiples dommages, notamment des dénis de service et l'exposition d'informations. Cette révision met à jour plusieurs informations, dont la liste des produits affectés.

http://www.cisco.com/warp/public/707/cisco-sa-20070412-wlc.shtml

Révision du bulletin 82421

Cisco a révisé le bulletin 82421 concernant un manque de validation dans le système d'aide en ligne ('online help system') fourni avec plusieurs produits qui autorise un attaquant distant à mener des attaques de type "Cross-Site Scripting" contre un utilisateur. Cette révision met à jour la liste des produits vulnérables.

http://www.cisco.com/warp/public/707/cisco-sr-20070315-xss.shtml

FREEBSD

Disponibilité de plusieurs correctifs

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

ipv6 FreeBSD-SA-07:03

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

FREETYPE

Disponibilité de la version 2.3.3 de 'FreeType'

Le projet FreeType a annoncé la disponibilité de la version 2.3.3 du produit 'FreeType'. Cette nouvelle version corrige la faille récemment discutée, référencée CVE-2007-1351, qui permet d'exécuter du code arbitraire.

http://sourceforge.net/project/shownotes.php?group_id=3157&release_id=498954

CVE-2007-1351

HP

Correctifs 'BIND' et 'OpenSSL' pour 'Tru64 Unix'

HP a annoncé, dans le bulletin HPSBTU02207 (SSRT061213, SSRT061239, SSRT071304), la disponibilité de correctifs pour les produits 'BIND' et 'OpenSSL' sur HP 'Tru64 Unix' versions 5.1B-4, 5.1B-3, 5.1A PK6, 4.0G PK4 et 4.0F PK8, 'Internet Express' version 6.6 et 'Insight Management Agents for Tru64 UNIX'. Ils corrigent de multiples failles qui peuvent entraîner l'exécution de code arbitraire et des dénis de service.

http://www4.itrc.hp.com/service/cki/docDisplay.do?docId=c00967144

CVE-2006-2937, CVE-2006-2940, CVE-2006-3738, CVE-2006-4339, CVE-2007-0493, CVE-2007-0494

Correctifs pour 'CIFS Server' ('Samba')

HP a annoncé, dans le bulletin HPSBUX02204 (SSRT071341), la disponibilité de correctifs pour 'CIFS Server' ('Samba') sur HP-UX B.11.11, B.11.23 et B.11.31. Ils corrigent une erreur de codage dans le démon 'smbd' qui permet à un utilisateur distant, authentifié sur le serveur, d'épuiser les ressources processeur et mémoire (déni de service).

http://www4.itrc.hp.com/service/cki/docDisplay.do?docId=c00943462

CVE-2007-0452

Révision du bulletin HPSBMA02133 (SSRT061201)

HP a révisé le bulletin HPSBMA02133 (SSRT061201) concernant la vulnérabilité de HP 'Oracle for OpenView' à de nombreuses failles Oracle. Cette révision intègre les failles discutées dans le bulletin Oracle d'avril 2007. HP recommande l'application des correctifs Oracle.

http://www5.itrc.hp.com/service/cki/docDisplay.do?docId=c00727143

Vulnérabilité de 'SMA' à la faille MS07-014

HP a annoncé, dans le bulletin HPSBST02206 (SSRT071354), la vulnérabilité de 'Storage Management Appliance' I, II et III ('SMA') aux multiples failles Microsoft annoncées dans l'avis MS07-014. Ces failles qui affectent 'Word' peuvent être exploitées par un attaquant afin d'exécuter du code arbitraire avec les droits de l'utilisateur courant. HP préconise d'installer les différents correctifs Microsoft disponibles.

http://www5.itrc.hp.com/service/cki/docDisplay.do?docId=c00965724

CVE-2006-5994, CVE-2006-6456, CVE-2006-6561, CVE-2007-0208, CVE-2007-0209, CVE-2007-0515

Vulnérabilités MS07-018 à MS07-022 dans HP 'SMA'

HP a annoncé, dans le bulletin HPSBST02208 (SSRT071365), la vulnérabilité de 'Storage Management Appliance' I, II et III ('SMA') aux multiples failles Microsoft annoncées dans les avis MS07-018, MS07-019, MS07-020, MS07-021 et MS07-022. Ces failles peuvent être exploitées par un attaquant afin d'exécuter du code arbitraire, de provoquer un déni de service, d'obtenir des informations ou de mener des attaques de type "Cross-Site Scripting". HP préconise d'installer les différents correctifs Microsoft disponibles.

http://www5.itrc.hp.com/service/cki/docDisplay.do?docId=c00978780

CVE-2006-6696, CVE-2006-6797, CVE-2007-0938, CVE-2007-0939, CVE-2007-1204, CVE-2007-1205, CVE-2007-1206, CVE-2007-1209

IBM

Correctifs pour la faille Kerberos CVE-2007-1216

Une alerte postée sur le site Web du AusCERT (CERT Australien) annonce la vulnérabilité du produit 'Network Authentication Service' d'IBM à la faille 'Kerberos 5' référencée CVE-2007-1216. Les versions 1.3.0.0 à 1.3.0.5, et 1.4.0.0 à 1.4.0.5 du produit sont vulnérables. Cette faille, une double libération de la mémoire dans la bibliothèque 'GSS-API', permet à un attaquant distant d'exécuter du code arbitraire. Les versions 1.3.0.6 et 1.4.0.6 corrigent cette faille.

http://www.auscert.org.au/render.html?it=7456

CVE-2007-1216

KASPERSKY LABS

Disponibilité du "Maintenance Pack 2"

Kaspersky a annoncé la disponibilité du correctif "Maintenance Pack 2" pour les produits 'Kaspersky Anti-Virus' version 6.0 et 'Kaspersky Internet Security' version 6.0. Ce correctif corrige trois failles récemment discutées dans les produits 'Kaspersky Anti-Virus for File Server' et 'Kaspersky Anti-Virus for Workstations' qui peuvent permettre à un attaquant local ou distant d'exécuter du code arbitraire.

http://www.kaspersky.com/technews?id=203038694

LINUX DEBIAN

Disponibilité de nombreux correctifs

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

file	*DSA-1274*	*zope2.7*	*DSA-1275*	*krb5*	*DSA-1276*
XMMS	*DSA-1277*	*man-db*	*DSA-1278*	*webcalendar*	*DSA-1279*
aircrack	*DSA-1280*	*clamav*	*DSA-1281*	*php4*	*DSA-1282*

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 :

file			*Core6*	*FEDORA-2007:391*
krb5	*Core5*	*FEDORA-2007:409*	*Core6*	*FEDORA-2007:408*
openssh	*Core5*	*FEDORA-2007:395*	*Core6*	*FEDORA-2007:394*
evolution	*Core5*	*FEDORA-2007:404*	*Core6*	*FEDORA-2007:393*
ImageMagick			*Core6*	*FEDORA-2007:413*
libXFont	*Core5*	*FEDORA-2007:423*	*Core6*	*FEDORA-2007:422*
xorg	*Core5*	*FEDORA-2007:424*	*Core6*	*FEDORA-2007:425*
libX11	*Core5*	*FEDORA-2007:427*	*Core6*	*FEDORA-2007:426*
kernel	*Core5*	*FEDORA-2007:433*	*Core6*	*FEDORA-2007:432*
php			*Core6*	*FEDORA-2007:415*
ImageMagick	*Core5*	*FEDORA-2007:414*		
php	*Core5*	*FEDORA-2007:455*		

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 :

evolution	*MDKSA-2007:070*	*2007*		
xmms	*MDKSA-2007:071*		*CS3.0*	
kdelibs	*MDKSA-2007:072*	*2007*	*CS3.0*	*CS4.0*
openoffice	*MDKSA-2007:073*	*2007*	*CS3.0*	
qt3	*MDKSA-2007:074*	*2007*	*CS3.0*	*CS4.0*
qt4	*MDKSA-2007:075*	*2007*		

kdelibs	MDKSA-2007:076			2007	CS3.0	CS4.0	
krb5	MDKSA-2007:077		2006	2007	CS3.0	CS4.0	MNF2.0 kernel
MDKSA-2007:078		2007					
xorg	MDKSA-2007:079			2007	CS3.0	CS4.0	
tighvnc	MDKSA-2007:080			2007	CS3.0	CS4.0	
freetype2	MDKSA-2007:081			2007	CS3.0	CS4.0	MNF2.0
madwifi	MDKSA-2007:082			2007			
mod_perl	MDKSA-2007:083		2006	2007	CS3.0	CS4.0	
ipsec-tools	MDKSA-2007:084			2007		CS4.0	MNF2.0
freeradius	MDKSA-2007:085			2007		CS4.0	
cups	MDKSA-2007:086			2007	CS3.0	CS4.0	
php	MDKSA-2007:087				CS3.0		MNF2.0
php	MDKSA-2007:088					CS4.0	
php	MDKSA-2007:089			2007		CS4.0	
php	MDKSA-2007:090			2007.1			
sqlite	MDKSA-2007:091			2007	CS3.0	CS4.0	
freeradius	MDKSA-2007:092					CS4.0	
zziplib	MDKSA-2007:093					CS4.0	
postgresql	MDKSA-2007:094			2007	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 :

krb5	RHSA-2006:0095-01				AS.ES.WS 5.0
xorg	RHSA-2006:0126-01			AS.ES.WS 4.0	
xfree86	RHSA-2006:0125-01	AS.ES.WS 2.1	AS.ES.WS 3.0		
mysql	RHSA-2006:0152-01			AS.ES.WS 4.0	
libXfont	RHSA-2006:0132-01				AS.ES.WS 5.0
squid	RHSA-2006:0131-0				AS.ES.WS 5.0
xorg	RHSA-2006:0127-01				AS.ES.WS 5.0
php	RHSA-2006:0162-01				
freetype	RHSA-2006:0150-01		AS.ES.WS 3.0	AS.ES.WS 4.0	AS.ES.WS 5.0
cups	RHSA-2006:0123-01		AS.ES.WS 3.0	AS.ES.WS 4.0	AS.ES.WS 5.0
x11	RHSA-2006:0157-01				AS.ES.WS 5.0
php	RHSA-2006:0155-01		AS.ES.WS 3.0	AS.ES.WS 4.0	
php	RHSA-2006:0154-01		AS.ES.WS 3.0	AS.ES.WS 4.0	AS.ES.WS 5.0
php	RHSA-2006:0153-01				AS.ES.WS 5.0
java.1.4.2.ibm	RHSA-2006:0166-01		AS.ES.WS 3.0	AS.ES.WS 4.0	
java.1.5.0.ibm	RHSA-2006:0167-01				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 :

gpg	SUSE-SA:2007:024		
krb5	SUSE-SA:2007:025		
clamav	SUSE-SA:2007:026		
xfree	SUSE-SA:2007:027		
opera	SUSE-SA:2007:028		
Summary Report 5	SR_2007_5	Summary Report 6	SR_2007_6
Summary Report 7	SR_2007_7		

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

MICROSOFT

Information additionnelle pour la faille des curseurs

Une information, relayée par F-Secure, annonce que Microsoft va publier un correctif le 03/04/2007 pour la récente faille découverte dans la gestion des curseurs animés. Cette faille permet, à l'aide d'un document HTML spécialement construit, d'exécuter du code arbitraire. Microsoft a aussi révisé son bulletin 935423 afin d'ajouter de nouvelles informations dans plusieurs sections.

http://www.f-secure.com/weblog/archives/archive-042007.html#00001159

http://www.microsoft.com/technet/security/bulletin/advance.mspx

CVE-2007-0038, CVE-2007-1765

Révision de l'alerte 935964

Microsoft a révisé l'alerte 935964 concernant un débordement de pile dans le service 'DNS' des plate-formes Windows. Cette faille permet d'exécuter du code arbitraire avec des droits privilégiés. Cette révision met à jour certaines informations, notamment dans la section "Suggested Actions". On peut noter que cette faille est actuellement exploitée sur Internet.

http://www.microsoft.com/technet/security/advisory/935964.mspx

CVE-2007-1748

NETSCAPE

Disponibilité de la version 8.1.3 de 'Netscape'

Netscape a annoncé la disponibilité de la version 8.1.3 du navigateur 'Netscape'. Cette nouvelle version corrige les failles Mozilla MFSA 2006-57 à MFSA 2006-67 qui peuvent entraîner, entre autres choses, des dénis de service et l'exécution de code arbitraire.

http://browser.netscape.com/ns8/security/alerts.jsp

CVE-2006-4253, CVE-2006-4565, CVE-2006-4566, CVE-2006-4567, CVE-2006-4568, CVE-2006-4569, CVE-2006-4570, CVE-2006-4571, CVE-2006-5462, CVE-2006-5463, CVE-2006-5464, CVE-2006-5747, CVE-2006-5748

NOVELL

Correctif pour la faille CVE-2007-0957

Novell a annoncé, dans le bulletin 3618705, la disponibilité de la version 1.0.2 de Novell KDC (Key Distribution Center). Cette version corrige la faille 'Kerberos 5', référencée CVE-2007-0957, dans la fonction 'krb5_klog_syslog()' qui permet d'exécuter du code arbitraire.

https://secure-support.novell.com/KanisaPlatform/Publishing/150/3618705_f.SAL_Public.html

CVE-2007-0957

OPENBSD

Correctifs pour 'IPv6'

Le projet OpenBSD a annoncé la disponibilité de correctifs pour 'IPv6' sur 'OpenBSD' versions 3.9 et 4.0. Ils corrigent une faille dans le traitement des en-têtes de routage 'Type 0' qui peut permettre à un attaquant distant de provoquer un déni de service. Il s'agit en fait d'une erreur de conception du protocole 'IPv6' lui même.

http://www.openbsd.org/errata40.html#012_route6

http://www.openbsd.org/errata39.html#022_route6

Correctifs pour 'X.org'

Le projet OpenBSD a annoncé la disponibilité de correctifs pour 'X.org' sur 'OpenBSD' versions 3.9 et 4.0. Ils corrigent de multiples failles qui peuvent permettre à un attaquant d'exécuter du code arbitraire avec des privilèges élevés.

http://www.openbsd.org/errata40.html#011_xorg

http://www.openbsd.org/errata39.html#021_xorg

CVE-2007-1003, CVE-2007-1351, CVE-2007-1352, CVE-2007-1667

ORACLE

Révision du bulletin Oracle d'avril 2007

Oracle a révisé son bulletin d'avril 2007 concernant de nombreuses vulnérabilités dans plusieurs produits. Cette révision met à jour plusieurs sections.

http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuapr2007.html

SGI

Correctif cumulatif #73 pour SGI ProPack 3 SP6

SGI a annoncé, dans le bulletin 20070401-01-P, la disponibilité du correctif cumulatif "Security Update #73" (correctif 10389) pour SGI ProPack 3 SP6 sur plate-forme Altix. Il corrige trois failles dans 'Kerberos 5' qui autorisent un attaquant distant à exécuter du code arbitraire et à obtenir un accès non autorisé sur une machine vulnérable.

ftp://patches.sgi.com/support/free/security/advisories/20070401-01-P.asc

CVE-2007-0956, CVE-2007-0957, CVE-2007-1216

SUN

Correctifs pour les failles dans la bibliothèque 'NSS'

Sun a annoncé, dans le document 102856, la disponibilité de correctifs pour les produits Sun Java Enterprise System et Sun Solaris, corrigeant les failles référencées CVE-2007-0008 et CVE-2007-0009 dans la bibliothèque 'NSS'. Ces deux failles, des débordements de pile et de buffer, peuvent entraîner l'exécution de code arbitraire.

http://sunsolve.sun.com/search/document.do?assetkey=1-26-102856-1

CVE-2007-0008, CVE-2007-0009

Correctifs pour 'libX11' sur 'Solaris'

Sun a annoncé, dans le bulletin 102888, la disponibilité de correctifs pour la bibliothèque 'libX11' sur les plate-formes 'Solaris' version 8, 9 et 10. Ils corrigent de multiples débordements d'entier qui peuvent permettre à un attaquant distant de provoquer des dénis de service ou d'exécuter du code arbitraire.

http://sunsolve.sun.com/search/document.do?assetkey=1-26-102888-1

CVE-2007-1667

Correctifs pour 'Mozilla'

Sun a annoncé, dans le bulletin 102865, la disponibilité de correctifs pour 'Mozilla' sur les plate-formes 'Solaris' versions 8, 9 et 10. Ils corrigent de multiples vulnérabilités, dont un débordement d'entier, dans le moteur 'JavaScript' du navigateur 'Mozilla' qui peuvent entraîner l'exécution de code arbitraire.

http://sunsolve.sun.com/search/document.do?assetkey=1-26-102865-1

CVE-2006-3805

Faille CVE-2006-6497 dans 'Mozilla' sur Solaris

Sun a annoncé, dans le bulletin 102885, la vulnérabilité du navigateur 'Mozilla' version 1.7 fourni avec 'Solaris' versions 8, 9 et 10, à la faille référencée CVE-2006-6497. Elle permet d'exécuter du code arbitraire ou de provoquer un déni de service du produit. Sun fournit des correctifs temporaires.

http://sunsolve.sun.com/search/document.do?assetkey=1-26-102885-1

CVE-2006-6497

Faille CVE-2007-0002 dans 'StarOffice' et 'StarSuite'

Sun a annoncé, dans le bulletin 102863, la vulnérabilité des produits 'StarOffice' et 'StarSuite', version 8, à la faille référencée CVE-2007-0002. Elle permet d'exécuter du code arbitraire. Des correctifs sont disponibles dans l'avis original.

http://sunsolve.sun.com/search/document.do?assetkey=1-26-102863-1

CVE-2007-0002

Publication du document 102867

Sun a publié le document 102867 concernant la vulnérabilité du produit Sun 'SEAM' versions 1.0.1 et 1.0.2 (Sparc et x86) à la faille affectant le démon 'telnetd' de 'Kerberos 5'. Cette faille autorise un attaquant distant à obtenir un accès non autorisé à une machine vulnérable. Il n'y a pas de correctif officiel actuellement disponible.

http://sunsolve.sun.com/search/document.do?assetkey=1-26-102867-1

CVE-2007-0956

Révision de l'alerte 102696

Sun a révisé l'alerte 102696 concernant la faille 'OpenSSL' référencée CVE-2006-4339 qui affecte certains serveurs Web Sun et qui permet à un attaquant de forger des signatures RSA de type 'PKCS #1 v1.5'. Cette révision annonce la mise à jour des sections "Contributing Factors" et "Resolution".

http://sunsolve.sun.com/search/document.do?assetkey=1-26-102696-1

CVE-2006-4339

Révision de l'alerte 102794

Sun a révisé le bulletin 102794 concernant la vulnérabilité des produits 'StarOffice' et 'StarSuite' à la faille référencée CVE-2007-0238 qui peut entraîner l'exécution de commandes arbitraires. Cette révision met à jour les sections "Contributing Factors" et "Resolution".

http://sunsolve.sun.com/search/document.do?assetkey=1-26-102794-1

CVE-2007-0238

Révision de l'avis 102807

Sun a révisé le bulletin 102807 concernant la vulnérabilité des produits 'StarOffice' et 'StarSuite' à la faille référencée CVE-2007-0239 qui peut entraîner l'exécution de code arbitraire. Cette révision met à jour les sections "Contributing Factors" et "Resolution".

http://sunsolve.sun.com/search/document.do?assetkey=1-26-102807-1

CVE-2007-0239

Révision des bulletins 102807 et 102794

Sun a révisé les bulletins 102807 et 102794 concernant la vulnérabilité des produits 'StarOffice' et 'StarSuite' versions 6, 7 et 8 aux failles référencées CVE-2007-0239 et CVE-2007-0238. Elles permettent d'exécuter des commandes et du code arbitraire. Ces révisions mettent à jour les sections "Contributing Factors" et "Resolution" en annonçant la disponibilité de correctifs, et clos ces bulletins.

http://sunsolve.sun.com/search/document.do?assetkey=1-26-102794-1

http://sunsolve.sun.com/search/document.do?assetkey=1-26-102807-1

CVE-2007-0238, CVE-2007-0239

Révision du bulletin 101338 (anciennement 56720)

Sun a révisé le bulletin 101338 (anciennement 56720) concernant une faille dans 'XScreenSaver' qui ne verrouille pas l'écran en environnement GNOME pour les utilisateurs 'root'. Cette révision met à jour les sections "Contributing Factors" et "Resolution", et clos le bulletin.

http://sunsolve.sun.com/search/document.do?assetkey=1-26-101338-1

Révision du bulletin 102294

Sun a révisé le bulletin 102294 concernant la vulnérabilité des annuaires LDAP 'Sun ONE Directory Server' et 'Sun Java System Directory Server' à une faille qui peut entraîner un déni de service d'un serveur vulnérable. Cette révision met à jour la section "Resolution".

http://sunsolve.sun.com/search/document.do?assetkey=1-26-102294-1

CVE-2006-0647

Révision du bulletin 102696

Sun a révisé l'alerte 102696 concernant la faille 'OpenSSL' référencée CVE-2006-4339 qui affecte certains serveurs Web Sun et qui permet à un attaquant de forger des signatures RSA de type 'PKCS #1 v1.5'. Cette révision annonce la mise à jour des sections "Contributing Factors" et "Resolution".

http://sunsolve.sun.com/search/document.do?assetkey=1-26-102696-1

CVE-2006-4339

Révision du bulletin 102720

Sun a révisé le bulletin 102720 concernant la vulnérabilité des plate-formes Sun 'Solaris' version 10 et Sun 'JDS release 2' à la faille CVE-2006-3404, affectant 'gimp' qui peut entraîner un déni de service et l'exécution de code arbitraire. Cette révision annonce la mise à jour de la section "Relief/Workaround".

http://sunsolve.sun.com/search/document.do?assetkey=1-26-102720-1

CVE-2006-3404

Révision du bulletin 102747

Sun a révisé le bulletin 102747 concernant la vulnérabilité du système Sun 'Solaris' version 10 aux failles 'OpenSSL' référencées CVE-2006-2937 et CVE-2006-2940 qui peuvent entraîner des dénis de services du système. Cette révision annonce la mise à jour des sections "Contributing Factors" et "Resolution".

http://sunsolve.sun.com/search/document.do?assetkey=1-26-102747-1

CVE-2006-2937, CVE-2006-2940

Révision du bulletin 102759

Sun a révisé le bulletin 102759 concernant la vulnérabilité de 'Solaris WAN Boot' sur 'Solaris' versions 9 et 10 à la faille 'OpenSSL' référencée CVE-2006-4339 quipermet à un attaquant de forger des signatures de type 'PKCS #1 v1.5'. Cette révision annonce la mise à jour des sections "Contributing Factors" et "Resolution".

http://sunsolve.sun.com/search/document.do?assetkey=1-26-102759-1

CVE-2006-4339

Révision du bulletin 102781

Sun a révisé le bulletin 102781 concernant des failles dans le navigateur 'Mozilla' sur Sun 'Solaris' versions 8, 9 et 10 qui peuvent permettent de contourner certains mécanismes de sécurité. Sun a mis à jour les sections "Contributing Factors" et "Resolution", et clos le bulletin.

http://sunsolve.sun.com/search/document.do?assetkey=1-26-102781-1

CVE-2006-4340, CVE-2006-5462

Révision du bulletin 102800

Sun a révisé le bulletin 102800 concernant la vulnérabilité du navigateur 'Mozilla' version 1.7, sur 'Solaris' versions 8, 9 et 10, aux failles référencées CVE-2006-6505 et CVE-2006-2776. Ces vulnérabilités permettent d'obtenir des droits privilégiés et de contourner certains mécanismes de sécurité. 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=1-26-102800-1

CVE-2006-2776, CVE-2006-6505

Révision du bulletin 102828

Sun a révisé le bulletin 102828 concernant une faille dans les produits 'Sun Fire X2100M2' et 'Sun Fire X2200M2' qui autorise un utilisateur à obtenir des droits privilégiés sur un produit vulnérable. Cette révision annonce la mise à jour des sections "Synopsis" et "Impact".

http://sunsolve.sun.com/search/document.do?assetkey=1-26-102828-1

Révision du bulletin 102846

Sun a révisé le bulletin 102846 concernant une erreur de codage qui affecte la fonction 'js_dtoa()' de 'Mozilla', qui peut permettre à un attaquant distant de provoquer un déni de service. Cette révision met à jour les sections "Contributing Factors" et "Resolution", et clos l'alerte.

http://sunsolve.sun.com/search/document.do?assetkey=1-26-102846-1

CVE-2006-6499

Révision du bulletin 102865

Sun a révisé le bulletin 102865 concernant de multiples vulnérabilités dans le moteur 'JavaScript' du navigateur 'Mozilla' qui peuvent entraîner l'exécution de code arbitraire. Cette révision met à jour les sections "Contributing Factors" et "Resolution", et clos le bulletin.

http://sunsolve.sun.com/search/document.do?assetkey=1-26-102865-1

CVE-2006-3805

Révision du bulletin 102867

Sun a révisé le bulletin 102867 concernant une faille dans le démon 'telnetd' de 'Kerberos 5', fourni avec Sun 'SEAM' versions 1.0.1 et 1.0.2. Cette faille autorise un attaquant à obtenir un accès non autorisé à une machine vulnérable. Cette révision met à jour les sections "Contributing Factors" et "Resolution" en annonçant la disponibilité de correctifs, et clos le bulletin.

http://sunsolve.sun.com/search/document.do?assetkey=1-26-102867-1

CVE-2007-0956

Révision du bulletin 102885

Sun a révisé le bulletin 102885 concernant la vulnérabilité du navigateur 'Mozilla' version 1.7 fourni avec 'Solaris' versions 8, 9 et 10, à la faille référencée CVE-2006-6497 qui permet d'exécuter du code arbitraire ou de provoquer un déni de service du produit. Cette révision annonce la mise à jour des sections "Contributing Factors" et "Resolution".

http://sunsolve.sun.com/search/document.do?assetkey=1-26-102885-1

CVE-2006-6497

Vulnérabilité CVE-2007-2138 de 'Solaris' version 10

Sun a annoncé, dans le bulletin 102894, la vulnérabilité de la plate-forme 'Solaris' version 10 à la faille 'PostgreSQL' référencée CVE-2007-2138. Cette vulnérabilité qui affecte les fonctions de type 'SECURITY DEFINER' peut permettre à un utilisateur malveillant d'obtenir des privilèges élevés.

http://sunsolve.sun.com/search/document.do?assetkey=1-26-102894-1

CVE-2007-2138

Vulnérabilités de 'Xsun' et 'Xorg' sur 'Solaris'

Sun a annoncé, dans le bulletin 102886, la vulnérabilité des serveurs 'Xsun' et 'Xorg' sur les plate-formes 'Solaris' versions 8, 9 et 10 aux failles référencées CVE-2007-1003, CVE-2007-1351 et CVE-2007-1352. Elles permettent à un attaquant d'exécuter du code arbitraire avec des privilèges élevés. Il n'y a pas de correctif officiel actuellement disponible.

http://sunsolve.sun.com/search/document.do?assetkey=1-26-102886-1

CVE-2007-1003, CVE-2007-1351, CVE-2007-1352

US-CERT

Reprise de l'avis Apple Security Update 2007-004

L'US-CERT a repris, sous la référence TA07-109A, l'avis Apple Security Update 2007-004 concernant de multiples failles dans divers composants de 'Mac OS X' et 'Mac OS X Server' versions 10.3.9 et 10.4.9. Ces failles peuvent entraîner, entre autres choses, des dénis de service d'applications et l'exécution de code arbitraires.

http://www.uscert.gov/cas/techalerts/TA07-109A.html

CVE-2006-0300, CVE-2006-5867, CVE-2006-6143, CVE-2006-6652, CVE-2007-0022, CVE-2007-0465, CVE-2007-0646, CVE-2007-0724, CVE-2007-0725, CVE-2007-0729, CVE-2007-0732, CVE-2007-0734, CVE-2007-0735, CVE-2007-0736, CVE-2007-0737, CVE-2007-0738, CVE-2007-0739, CVE-2007-0741, CVE-2007-0742, CVE-2007-0743, CVE-2007-0744, CVE-2007-0746, CVE-2007-0747, CVE-2007-0957, CVE-2007-1216

Reprise de l'avis Microsoft 935423

L'US-CERT a repris, sous la référence TA07-089A, l'avis Microsoft 935423 concernant une faille dans la gestion des curseurs animés des plate-formes Windows qui peut entraîner l'exécution de code arbitraire sur une plate-forme vulnérable.

http://www.us-cert.gov/cas/techalerts/TA07-089A.html

CVE-2007-0038

Reprise de l'avis Microsoft 935964

L'US-CERT a repris, sous la référence TA07-103A, l'avis Microsoft 935964 concernant un débordement de pile déclenché via l'interface 'RPC' du service 'DNS' des plate-formes Windows qui peut entraîner l'exécution de code arbitraire.

http://www.us-cert.gov/cas/techalerts/TA07-103A.html

CVE-2007-1748

Reprise de l'avis Microsoft MS07-017

L'US-CERT a repris, sous la référence TA07-093A, l'avis Microsoft MS07-017 concernant de multiples failles dans les plate-formes Windows qui peuvent entraîner l'exécution de code arbitraire locale ou distante.

http://www.us-cert.gov/cas/techalerts/TA07-093A.html

CVE-2006-5586, CVE-2006-5758, CVE-2007-0038, CVE-2007-1211, CVE-2007-1212, CVE-2007-1213, CVE-2007-1215

Reprise de l'avis Oracle d'avril 2007

L'US-CERT a repris, sous la référence TA07-108A, l'avis Oracle d'avril 2007 concernant de nombreuses failles dans les produits Oracle qui peuvent entraîner de multiples dommages.

http://www.uscert.gov/cas/techalerts/TA07-108A.html

Reprise des avis Microsoft d'avril 2007

L'US-CERT a repris, sous la référence TA07-100A, les bulletins Microsoft d'avril 2007 concernant de multiples failles dans Windows, Content Management Server et Internet Explorer qui peuvent entraîner, entre autres choses, l'exécution de code arbitraire et des dénis de service.

http://www.us-cert.gov/cas/techalerts/TA07-100A.html

Reprise des avis MIT du 03/04/2007

L'US-CERT a repris, sous la référence TA07-093B, les avis MIT MITKRB5-SA-2007-001, MITKRB5-SA-2007-002 et MITKRB5-SA-2007-003 concernant de multiples failles dans le produit 'Kerberos 5' qui peuvent entraîner l'exécution de code arbitraire et autoriser un attaquant distant à obtenir un accès non autorisé.

http://www.us-cert.gov/cas/techalerts/TA07-093B.html

CVE-2007-0956, CVE-2007-0957, CVE-2007-1216

VMWARE

Correctifs pour 'ESX Server'

VMWare a annoncé, dans le bulletin VMSA-2007-0002, la disponibilité de correctifs pour 'ESX Server' versions 2.0.2, 2.1.3, 2.5.3, 2.5.4, 3.0.0 et 3.0.1. Ils corrigent de multiples failles qui peuvent entraîner, entre autres choses, des dénis de service et l'exécution de code arbitraire.

http://lists.grok.org.uk/pipermail/full-disclosure/2007-March/053268.html

CVE-2006-3739, CVE-2006-3740, CVE-2006-4334, CVE-2006-4335, CVE-2006-4336, CVE-2006-4337, CVE-2006-4338, CVE-2006-6097

Correctifs pour 'ESX Server'

VMWare a annoncé, dans le bulletin VMSA-2007-0003, la disponibilité de correctifs pour 'ESX Server' versions 3.0.0 et 3.0.1. Ils corrigent de multiples failles qui peuvent entraîner des dénis de service, l'exécution de code arbitraire et la corruption de données arbitraires.

http://lists.grok.org.uk/pipermail/full-disclosure/2007-April/053483.html

CVE-2003-0107, CVE-2005-1704, CVE-2005-1849, CVE-2005-2096, CVE-2005-3011, CVE-2006-4810, CVE-2007-1270, CVE-2007-1271

CODES D'EXPLOITATION

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

CA

Code d'exploitation 'Brightstor ARCserve Backup'

Un code d'exploitation a été posté sur le site Web Milw0rm, exploitant une des failles discutées dans un précédent bulletin qui affecte les produits 'BrightStor ARCserve Backup'. Cette vulnérabilité peut entraîner l'exécution de code arbitraire. Ce code permet d'obtenir un interpréteur de commande sur le port TCP/4444.

http://www.milw0rm.com/exploits/3604

CVE-2006-5171

MICROSOFT

Codes d'exploitation pour la faille Microsoft 'DNS'

Deux codes d'exploitation ont été publiés sur le site Web Milw0rm. Ils exploitent la faille Microsoft référencée 935964. Elle permet, via un débordement de pile dans le serveur 'DNS' des plate-formes Windows, de provoquer l'exécution de code arbitraire. Ces codes permettent d'obtenir à distance un interpréteur de commandes.

http://milw0rm.com/exploits/3740

http://milw0rm.com/exploits/3746

CVE-2007-1748

BULLETINS ET NOTES

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

OPERA

Disponibilité de la version 9.20 du navigateur 'Opera'

Opera a annoncé la disponibilité de la version 9.20 du navigateur 'Opera'. Cette version corrige un problème dans la gestion de la propriété 'charset' qui autorise un attaquant distant, à l'aide d'un site Web malicieux, de mener des attaques de type "Cross-Site Scripting".

http://www.opera.com/support/search/view/855/

MICROSOFT

Message piégé concernant 'Internet Explorer'

Différentes sources annoncent qu'un message piégé concernant le navigateur Web Microsoft 'Internet Explorer' version 7 est actuellement diffusé. Le message, supposé venir de Microsoft ('admin@microsoft.com'), propose aux utilisateurs de télécharger la version Beta 2 du navigateur. Il s'agit en réalité d'un virus qui est pour le moment encore mal identifié par les différents anti-virus. Il a été référencé par F-Secure et Kaspersky sous le nom de 'Virus.Win32.Grum.a'.

http://www.f-secure.com/weblog/archives/archive-032007.html#00001155

http://isc.sans.org/diary.html?storyid=2537

http://sunbeltblog.blogspot.com/2007/03/beware-fake-ie-7-downloads.html

WORDPRESS

Disponibilité de 'WordPress' version 2.1.3

Le projet WordPress a annoncé la disponibilité de la version 2.1.3. Elle corrige une faille qui permet d'injecter du code SQL arbitraire dans la base de données sous-jacente.

http://lists.grok.org.uk/pipermail/full-disclosure/2007-April/053564.html

http://wordpress.org/download/

ATTAQUES

OUTILS

NIRSOFT – MAIL PASSVIEW V1.38, SNIFFPASS V1.01 ET IPNETINFO V1.09

- **Description**

Le site '**NirSoft**' propose une multitude de petits outils Windows tous aussi remarquables et pratiques comme le faisait en son temps l'excellent site '**Sysinternals**'.

Développé par un certain '**Nir Sofer**', ces utilitaires partagent tous la même caractéristique: ils sont autonomes et d'une taille suffisamment raisonnable pour être installés à demeure sur une clef USB et ce d'autant qu'ils ne nécessitent aucune phase d'installation préalable.

Les 26 outils proposés sur le site sont regroupés en six catégories: '**Récupération de mot de passe**' (7), '**Outils de surveillance réseau**' (2), '**Utilitaires Internet**' (5), '**Utilitaires ligne de commande**' (1), '**Utilitaires Desktop**' (3) et '**Outils système**' (8). Parmi tous ceux-ci, trois outils apparaissent devoir impérativement figurer dans la boîte à outil de tout exploitant ou auditeur et méritent à ce titre d'être présentés plus en détail.

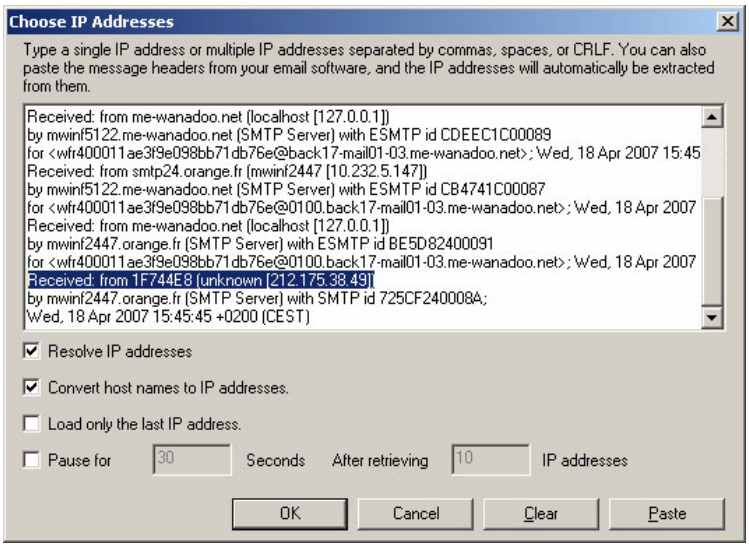
IPNetInfo

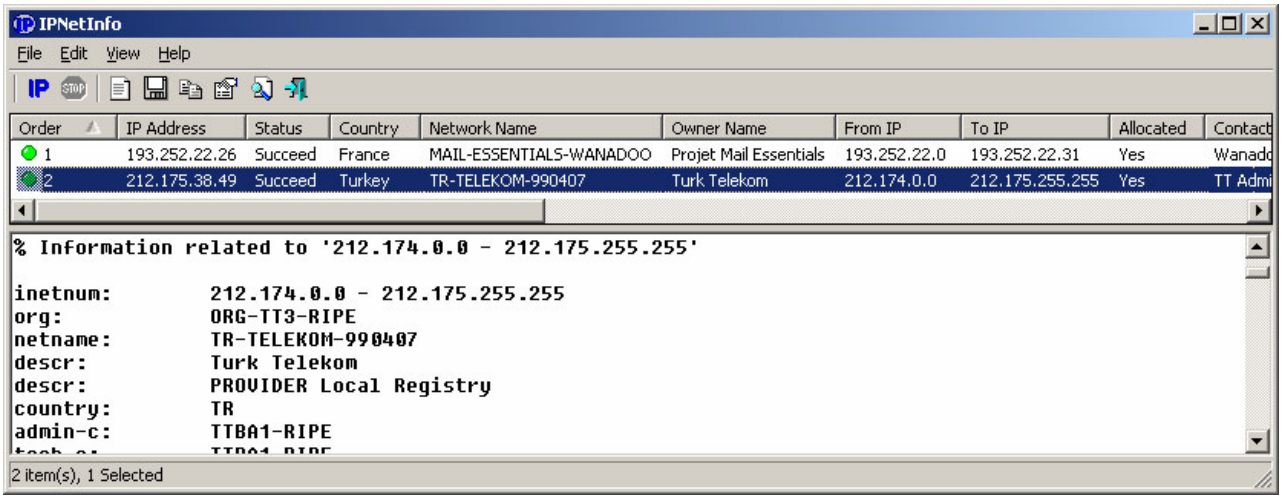
Cet utilitaire qui date déjà de 2005 deviendra rapidement tout aussi indispensable que peuvent l'être les célèbres sites '**DomainsDb**' ou '**DNSTools**'.

Il permet en effet de visualiser immédiatement, et sans autre manipulation, qu'un copier/coller toutes les informations disponibles dans les bases '**Whois**' à propos des adresses IP contenues dans le texte ayant été copié.

Son auteur l'a conçu pour faciliter l'analyse de l'en-tête des mails afin d'en identifier la provenance exacte. Il est cependant possible d'en détourner l'usage aucun contrôle n'étant effectué sur la structure du texte passé en copie.

IPNetInfo sera ainsi fort pratique pour assurer le référencement d'adresses IP contenues dans des sections de fichiers de journalisation qu'il suffira de copier dans la fenêtre prévue à cet usage.

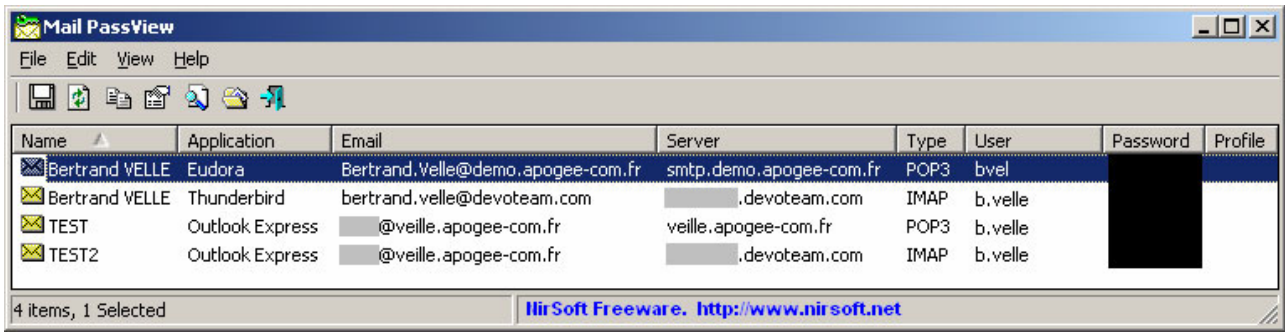




Mail Passview

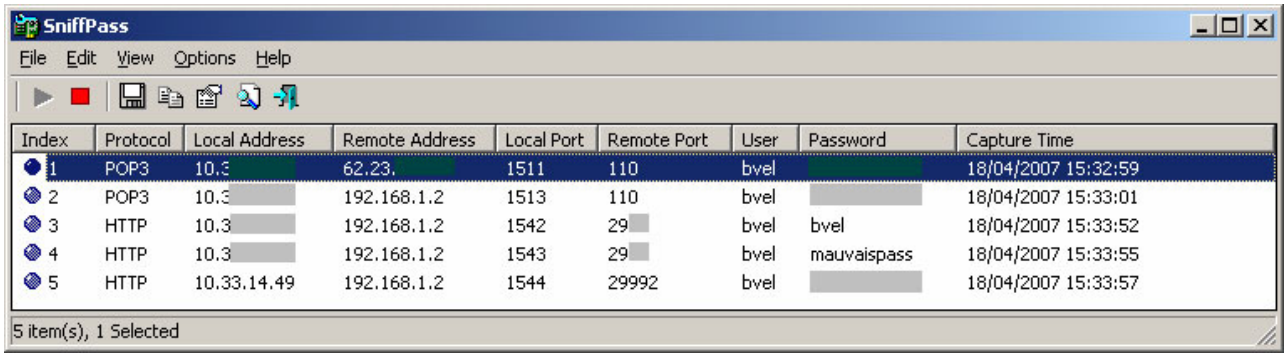
D'une simplicité extrême d'utilisation, cet utilitaire va parcourir les entrées de la base de registre et autres ressources du système pour en extraire les mots de passe stockés par les applications de messagerie ou les navigateurs.

La dernière version disponible est à même de traiter les structures utilisées par les applications suivantes: **Outlook Express**, **Outlook 2000** (services POP et SMTP uniquement), **Outlook 2002/2003** et **2007** (services POP, IMAP, HTTP et SMTP), **Windows Mail**, **IncrediMail**, **Eudora**, **Netscape 6** et **7**, **Thunderbird**, **Group Mail Free, Yahoo!Mail**, **HotMail/MSN Mail** et **GMail**.



Sniff Pass

L'utilitaire **SniffPass** vient compléter '**Mail Pass View**' en collectant directement les mots de passe transférés sur le réseau de rattachement du poste sur lequel il est exécuté. Une fonctionnalité somme toute classique mais dont l'implémentation en un unique exécutable de petite taille est bien utile.



On notera toutefois que l'utilitaire ne gère pas les codes d'erreur des différents protocoles reconnus et en conséquence collecte sans discrimination aucune toutes les données contenues dans la structure protocolaire réservée au transport du mot de passe !

Nous laisserons le soin au lecteur de découvrir les 23 autres outils proposés par **Nir Sofer**.

- **Complément d'information**

http://www.nirsoft.net/utils/mailpv.html	- Mail Password
http://www.nirsoft.net/utils/password_sniffer.html	- Password Sniffer
http://www.nirsoft.net/utils/ipnetinfo.html	- IpNet Info