

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2008-41

Conditions d'utilisation de ce document : <http://www.certa.ssi.gouv.fr/certa/apropos.html>
Dernière version de ce document : <http://www.certa.ssi.gouv.fr/site/CERTA-2008-ACT-041>

Gestion du document

Référence	CERTA-2008-ACT-041
Titre	Bulletin d'actualité 2008-41
Date de la première version	10 octobre 2008
Date de la dernière version	–
Source(s)	
Pièce(s) jointe(s)	Aucune

TAB. 1 – *Gestion du document*

Une gestion de version détaillée se trouve à la fin de ce document.

Le bulletin d'actualité est disponible dans son intégralité et au format PDF à l'adresse suivante :

<http://www.certa.ssi.gouv.fr/site/CERTA-2008-ACT-041.pdf>

Un extrait du bulletin, ne reprenant que les articles de la semaine, se trouve en HTML à l'adresse suivante :

<http://www.certa.ssi.gouv.fr/site/CERTA-2008-ACT-041/>

1 Incidents traités cette semaine

1.1 Des identifiants volés rendus publics

Cette semaine le CERTA a traité plusieurs incidents relatifs à la divulgation sur l'Internet d'identifiants FTP compromis. Plusieurs centaines de comptes FTP et les mots de passe associés ont été découverts. Ces identifiants, provenant certainement de plusieurs sources (attaques par dictionnaires, enregistreurs de frappe, ...), semblent avoir été exploités par des individus malintentionnés pour injecter dans des pages Web légitimes sur les serveurs compromis des codes malveillants de type *Neosploit*. Ces compromissions étaient peu visibles et n'ont pas attiré l'attention de certains administrateurs de site Web. Le CERTA recommande de :

- contrôler régulièrement l'intégrité des fichiers présents sur les serveurs ;
- limiter les connexions distantes aux adresses IP autorisées ;
- désactiver les services non utiles ;
- avoir une politique de mot de passe dits « forts » ;
- contrôler régulièrement les journaux des connexions pour mettre en évidence des attaques et des connexions non-désirées.

Dans le cas d'une compromission avérée, le CERTA recommande de suivre les règles de bonne conduite décrites dans la note d'information CERTA-2002-INF-002.

Documentation

- Note d'information du CERTA sur les bons réflexes en cas d'intrusion sur un système d'information : <http://www.certa.ssi.gouv.fr/site/CERTA-2002-INF-002/>

1.2 Compromission et rebonds

Le CERTA a traité cette semaine un incident, somme toute assez banal, mais qui permet de faire un rappel de certaines règles de sécurité essentielles.

Un serveur d'une administration a été compromis par un attaquant après une recherche exhaustive de mots de passe d'accès au service SSH, accessible depuis l'Internet. Une fois l'intrusion frauduleuse accomplie, l'attaquant a déposé un ensemble d'outils permettant d'utiliser le serveur compromis afin de conduire d'autres attaques par dictionnaire de mots de passe SSH.

Dans un premier temps, cet incident aurait pu être évité si les règles de l'art dans la construction des mots de passe avaient été respectées (voir la note d'information CERTA-2005-INF-001).

D'autre part, de l'aveu même de l'administrateur, le service SSH n'était utilisé que pour l'administration depuis le réseau interne. Il était donc légitime de filtrer au niveau du pare-feu les flux venant de l'Internet à destination de ce service. De même, les flux sortant à destination du port 22/tcp auraient dû être filtrés, ce qui aurait permis de bloquer les attaques conduites par rebond.

En résumé, cet incident nous permet de rappeler les règles suivantes :

- utiliser des mots de passe forts ;
- n'autoriser que ce qui est strictement nécessaire au niveau des flux entrants ;
- appliquer la même rigueur de filtrage au niveau des flux sortants ;
- journaliser aussi bien les flux entrants que les flux sortants.

2 Filoutage et ingénierie sociale

Une nouvelle méthode permettant la récupération des coordonnées bancaires et d'informations personnelles est apparue à la fin de cet été. Se présentant sous la forme d'un code malveillant, son installation permet d'inciter l'utilisateur victime à « activer » sa version de Microsoft Windows.

Imitant parfaitement la véritable fenêtre d'activation, le code malveillant demande les coordonnées bancaires tout en précisant qu'aucune transaction ne sera effectuée. Répondant au nom de *Kardphisher*, ce cheval de Troie permet l'envoi des données récoltées à un serveur distant.

Le CERTA rappelle qu'il est impératif de maintenir l'ensemble de son système d'information à jour (navigateur, antivirus, système d'exploitation, ...) afin de limiter l'installation « silencieuse » de ce type de programme. De plus, il ne faut jamais communiquer de coordonnées personnelles et/ou bancaires sans la certitude de la légitimité de la demande et l'assurance d'une transmission sécurisée de ces dernières vers une entité dûment authentifiée (ex: vérification des certificats). Dans le cas présent, le programme ne présente pas ces garanties. Enfin, ne jamais suivre de lien hypertexte ni ouvrir de pièce jointe provenant de courriel non sûr restent des précautions indispensables pour éviter toute installation de programme malveillant.

3 Les attaques en *Clickjacking*

Les médias ont beaucoup parlé cette semaine du *clickjacking* suite à l'annulation d'une présentation à la conférence **OWASP 2008** sur le sujet à la demande de la société Adobe, et cela afin de lui permettre de corriger les vulnérabilités affectant ses produits. Malheureusement, les attaques de ce type ne concernant pas que les produits d'Adobe, cet article est l'occasion de voir de quoi il s'agit et comment essayer de s'en protéger.

Comme son nom l'indique, il s'agit de détourner les *clicks* des utilisateurs pour leur faire exécuter des actions malgré eux. Ce nom ne désigne pas une vulnérabilité en particulier mais plutôt une faiblesse structurelle liée au fonctionnement du Web. Les utilisateurs font naturellement le parallèle entre appuyer sur un bouton visible et cliquer avec la souris, et n'imaginent pas qu'une multitude d'éléments invisibles peuvent s'intercaler « entre » le curseur et l'élément qu'ils visualisent en-dessous.

Les attaques en *clickjacking* se décomposent donc en deux étapes. La première concerne l'interception du *click*. La seconde est relative à l'utilisation de cette action à des fins malveillantes. Il existe de très nombreuses techniques pour détourner les actions de utilisateurs, que cela soit en utilisant des *iframes* transparentes qui recouvrent une page ou des *iframes* minuscules qui se déplacent avec le curseur. L'exemple suivant montre comment une section (balise *DIV*) peut être placée automatiquement sous le curseur (fonctionne avec *Firefox*).

```
<script language="JavaScript">
  function position(e) {
document.getElementById("dd").style.left = e.pageX-20;
document.getElementById("dd").style.top = e.pageY-5;
  }
document.onmousemove = position;
</script>
<div id="dd" style="position:absolute"> DIV sous la souris </div>
```

Une fois interceptés, les *clicks* reroutés sont utilisables dans le contexte de l'utilisateur et avec les droits de ce derniers, comme les attaques en *CSRF* (*Cross Site Request Forgery*). Donc tout ce que peut faire un utilisateur à l'aide d'un *click*, l'attaquant peut lui faire faire à son insu. Ainsi un programme *Flash* spécifiquement réalisé pouvait utiliser un *click* intercepté afin d'activer le micro ou la caméra de la machine, comme si l'utilisateur les avait volontairement mis en marche dans le cadre d'une vidéo-conférence (la version 10 de *Flash* corrige cette vulnérabilité). Le problème peut se poser du côté serveur si des actions sont réalisables d'un simple *click* (achats, transferts d'argent, ajout de contact de confiance, ...). Il est donc possible de limiter, au niveau des sites, les effets des attaques en demandant une action supplémentaire à l'utilisateur (code *pin*, *captcha*, ...). Du côté du client, limiter l'utilisation des scripts et des *iframe* permet de réduire les risques. Des fonctionnalités de sécurité empêchant de cliquer sur des éléments « cachés » commencent à être ajoutées aux navigateurs et aux modules de sécurité.

Documentation

- Bulletin de sécurité Adobe concernant l'activation du micro et de la caméra : <http://www.adobe.com/support/security/advisories/apsa08-08.html>
- Bulletin de sécurité CERTA-2008-AVI-490 : <http://www.certa.ssi.gouv.fr/site/CERTA-2008-AVI-490/index.html>
- Bulletin d'actualité du CERTA présentant la problématique des *iframes* : <http://www.certa.ssi.gouv.fr/site/CERTA-2007-ACT-025/index.html>
- Bulletin d'actualité du CERTA traitant des défigurations discrètes par injection d'*iframes* : <http://www.certa.ssi.gouv.fr/site/CERTA-2007-ACT-032/index.html>

4 Les boîtes à outils d'attaque

L'actualité a mis en avant la boîte à outils d'attaque *Neosploit*, mais le cas n'est pas isolé. *Mpack* a defrayer la chronique en juin 2007. D'autres kits sont utilisés avec plus ou moins d'écho dans les médias.

Certains outils sont verrouillés par leurs concepteurs, d'autres comme *Neosploit* ont un code source ouvert. Cela permet à des utilisateurs de traduire les interfaces utilisateur. Autre conséquence, la boîte à outils peut survivre à son équipe de développeurs. Ainsi, le 29 juillet 2008, les développeurs de *Neosploit* ont annoncé, par un message en russe, la fin des développements. La dernière version était alors la 3.0.7.

Dès le 9 août 2008, une version 3.1 de *Neosploit* réapparaît.

Ces boîtes à outils d'attaque comprennent deux volets qui correspondent à deux étages d'un système d'infection.

4.1 Modification de sites Web

Le premier volet consiste à compromettre des sites Web, très fréquentés si possible.

L'intrusion dans le site à modifier peut se faire de plusieurs manières :

- à l'aide d'un compte d'administration dont l'identifiant et le mot de passe peuvent être trouvés ou achetés sur l'Internet ;

- à l'aide d'un compte d'administration dont l'identifiant et le mot de passe sont recherchés par l'outil d'attaque (recherche par dictionnaire ou recherche exhaustive) ;
- à l'aide d'un compte d'administration dont l'identifiant et le mot de passe ont été récupérés par un enregistreur de frappes clavier ou tout autre programme malveillant de la même teneur ;
- à l'aide de vulnérabilités du site ou du serveur.

Une fois entré sur un site avec des droits d'administration, l'intrus insère dans les pages servies aux visiteurs du site des liens les orientant vers des sites malveillants. Ces liens peuvent se trouver dans beaucoup d'objets HTML. *MPack* faisait usage des cadres de type `iframe`, de taille infime (un pixel de côté) ou invisibles. Ils sont décrits dans le bulletin d'actualité CERTA-2007-ACT-025 du 22 juin 2007. Il est fréquent que le lien ne soit pas en clair mais calculé par des `javascripts` plus ou moins obscurcis (*obfuscated*). Ils sont décrits dans le bulletin d'actualité CERTA-2007-ACT-032 du 10 août 2007. Le script qui déchiffre reconstruit un lien ou un autre `javascript` dont l'apparence initiale est une chaîne aléatoire. Ce script est exécuté à son tour.

Quelques indices peuvent trahir la présence de tels scripts :

- des suites d'instructions comme `<script>document.write(unescape("%3Cscript%3E... ;`
- des chaînes de caractères d'apparence aléatoires ;
- le positionnement du code, tout en bas de la page, après beaucoup de retours à la ligne ou très à droite pour ne pas être visible sur un écran de largeur ordinaire ;
- une connexion inattendue lors de la consultation du site légitime.

4.2 Infection des ordinateurs des internautes

L'internaute qui visite le site compromis est amené à suivre automatiquement des connexions vers des sites malveillants. Généralement le lien aboutit à un site qui lui-même renvoie vers un autre site. De rebond en rebond l'internaute est conduit jusqu'au site contenant la « charge utile ».

Ce site est souvent sous le contrôle du développeur de la boîte à outils. Il contient divers codes malveillants ce qui permet d'adapter l'infection du poste de l'internaute à sa configuration :

- système d'exploitation, version, langue ;
- navigateur, logiciels installés comme les lecteurs multimédia et les suites de bureautique ;
- adresse IP, par exemple pour rester dissimulé si l'internaute trop curieux revient sur le site.

Les codes d'exploitation des vulnérabilités au catalogue sont variées :

- contre la suite *Microsoft Office* ;
- contre les lecteurs multimédia, comme *Quicktime* ou *Windows Media Player* ;
- contre les lecteurs de fichiers PDF, en recrudescence actuellement ;
- contre les navigateurs et les systèmes d'exploitation.

L'utilisateur de la boîte à outils, conducteur de l'infection, dispose de statistiques sur les ordinateurs compromis, les adresses IP, les quantités par pays, par système d'exploitation ou par code d'exploitation utilisé.

4.3 Recommandations

4.3.1 Recommandations pour les administrateurs de site

Les administrateurs de site doivent veiller à leur intégrité :

- par la mise à jour des logiciels utilisés ;
- par la configuration restrictive du système et des logiciels ;
- par une politique rigoureuse des mots de passe d'administration (complexité, longueur, durée de vie) ;
- par une bonne hygiène des postes utilisés pour administrer les sites ;
- par une surveillance régulière du contenu et de la configuration ;
- par la surveillance des journaux d'événements et de connexion.

4.3.2 Recommandations pour les internautes

Les internautes offriront une moindre surface d'attaque en :

- ayant un système d'exploitation, des logiciels et des extensions, notamment de navigateur, à jour ;
- ayant une configuration restrictive du système et des logiciels (pare-feu, désactivation des fonctions non utilisées) ;

- naviguant avec des droits limités, pas en administrateur ;
- n'autorisant l'exécution des codes mobiles, dont les javascripts, que lorsque cela est indispensable et après s'être assuré de l'inocuité des sites.

5 Projecteurs et fonctionnalités détournées

Certains modèles de projecteurs possèdent des fonctionnalités avancées allant au delà du simple affichage sur un écran de projection et des corrections optiques classiques (orientation, positionnement ou réglage du trapèze). En particulier, le CERTA a rencontré, lors d'une présentation, un projecteur doté d'un économiseur d'écran s'activant à chaque changement de résolution, lors d'un débranchement du câble vidéo ou au bout d'une période d'inactivité prolongée. Il s'agit bien ici d'une fonctionnalité du projecteur ne dépendant pas du tout du système d'exploitation de l'ordinateur qui y est branché. Or, si par défaut, cet économiseur affiche le logo du fabricant, il est possible pour l'utilisateur, grâce à un menu avancé, de prendre une capture d'écran de ce qui est projeté et d'en faire ce qui sera affiché lors du déclenchement de l'économiseur. Sur le modèle manipulé, il n'était possible de stocker qu'une seule image, mais l'« intelligence » y est. Il est donc, en théorie, possible pour ce simple périphérique d'affichage de stocker les informations projetées sous forme d'image dans une mémoire qui lui est propre. On peut dès lors imaginer que, sur les modèles haut-de-gamme, on pourra stocker un nombre plus important de clichés ou même enregistrer une petite vidéo.

Cette fonctionnalité peut donc avoir quelques conséquences en termes de confidentialité. Car, si elle est mise en œuvre, comment est-il possible de s'assurer que rien n'est stocké à l'insu de l'utilisateur ? Et lorsque le produit doit retourner en maintenance chez le fabricant, comment s'assurer qu'aucune information sensible n'est stockée dans l'appareil ? Il est à noter que cette technologie pourrait être appliquée à tout autre type de périphérique d'affichage comme de simples écrans.

Recommandations :

Le CERTA recommande, lors de l'achat de ce type de matériel, de s'assurer qu'il n'embarque pas ce type de fonctionnalité en particulier s'il doit être déployé dans un environnement sensible.

6 Mise à jour d'alertes

Cette semaine, le CERTA a mis à jour trois alertes publiées entre 2006 et 2007 :

- l'alerte CERTA-2006-ALE-012 concernant Microsoft PowerPoint qui a été réévaluée car le risque n'inclut plus une exécution de code arbitraire ;
- l'alerte CERTA-2007-ALE-007 concernant Windows Explorer qui a aussi été réévaluée car le risque n'inclut plus une exécution de code arbitraire ;
- l'alerte CERTA-2007-ALE-011 concernant Microsoft IIS dont les produits affectés, la description et les contournements ont été mis à jour.

Les vulnérabilités décrites dans les deux premières alertes ne sont pas pour autant corrigées, même si les documents apparaissent ainsi sur le site. La troisième alerte est toujours active.

Les lecteurs sont invités à consulter ces alertes sur le site du CERTA pour plus de détails.

Documentation

- Alerte CERTA-2006-ALE-012 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2006-ALE-012/index.html>
- Alerte CERTA-2007-ALE-007 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-007/index.html>
- Alerte CERTA-2007-ALE-011 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2006-ALE-011/index.html>

7 Ports observés

Le tableau 3 et la figure 1 montrent les rejets pour les ports sous surveillance que nous avons constatés sur des dispositifs de filtrage, entre le 02 et le 09 octobre 2008.

8 Liens utiles

- Mémento sur les virus :
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-002/>
- Note d'information du CERTA sur l'acquisition de correctifs :
<http://www.certa.ssi.gouv.fr/site/CERTA-2001-INF-004/>
- Note d'information du CERTA sur les systèmes obsolètes :
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-003/>
- Note d'information du CERTA sur les bonnes pratiques concernant l'hébergement mutualisé :
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-005/>
- Note d'information du CERTA sur les mots de passe :
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-001/>
- Note d'information sur la terminologie d'usage au CERTA :
<http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-002/>
- Note d'information du CERTA sur les enjeux de sécurité liés à une migration vers IPv6 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-004/>
- Unix security checklist version 2.0 du 8 octobre 2001 (Publication du CERT australien) :
<http://www.auscert.org.au/render.html?it=1935>
- Note d'information du CERTA sur les risques associés aux clés USB :
<http://www.certa.ssi.gouv.fr/site/CERTA-2000-INF-006/>
- Note d'information du CERTA sur les outils d'indexation et de recherche :
<http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-009/>
- Note d'information du CERTA sur la gestion des noms de domaine :
<http://www.certa.ssi.gouv.fr/site/CERTA-2007-INF-001/>
- Note d'information du CERTA sur le bon usage de PHP :
<http://www.certa.ssi.gouv.fr/site/CERTA-2007-INF-002/>

9 Rappel des avis émis

Dans la période du 03 au 10 octobre 2008, le CERTA a émis les avis suivants :

- CERTA-2008-AVI-480 : Vulnérabilités dans Novell eDirectory
- CERTA-2008-AVI-481 : Vulnérabilité dans Juniper NetScreen
- CERTA-2008-AVI-482 : Vulnérabilités dans Trend Micro
- CERTA-2008-AVI-483 : Multiples vulnérabilités dans des produits VMware
- CERTA-2008-AVI-484 : Vulnérabilité dans pam_krb5
- CERTA-2008-AVI-485 : Multiples vulnérabilités dans MPlayer
- CERTA-2008-AVI-486 : Vulnérabilité dans le protocole ndp de IPv6
- CERTA-2008-AVI-487 : Vulnérabilités dans Opera

Durant la même période, les avis suivants ont été mis à jour :

- CERTA-2007-AVI-377-001 : Vulnérabilité dans GNU tar
(ajout des références aux bulletins de sécurité Gentoo, Debian, Mandriva, SuSE, Ubuntu, FreeBSD et Avaya)
- CERTA-2007-AVI-391-003 : Vulnérabilité dans GNU Tar
(ajout des références aux bulletins de sécurité Ubuntu, Debian et Gentoo)
- CERTA-2008-AVI-392-001 : Multiples vulnérabilités dans Apache Tomcat
(ajout des références aux distributions Linux)
- CERTA-2008-AVI-461-001 : Vulnérabilité de FreeBSD
(ajout de la référence CVE)
- CERTA-2008-AVI-468 : Vulnérabilité dans Sun Solaris
(ajout des références au bulletin de sécurité Avaya et au bulletin CVE)
- CERTA-2008-AVI-479-001 : Multiples vulnérabilités dans Lighttpd
(ajout de vulnérabilités et des références CVE)

10 Actions suggérées

10.1 Respecter la politique de sécurité

La Politique de Sécurité des Systèmes d'Information (PSSI) est l'ensemble formalisé dans un document applicable, des directives, procédures, codes de conduite, règles organisationnelles et techniques, ayant pour objectif la protection des systèmes d'information de l'organisme. Elle traduit la reconnaissance officielle de l'importance accordée par la direction générale de l'organisme à la sécurité de ses systèmes d'information. D'une manière générale, elle contient une partie relative aux éléments stratégiques de l'organisme (périmètre, contexte, enjeux, orientations stratégiques en matière de SSI, référentiel réglementaire, échelle de sensibilité, besoins de sécurité, menaces) et une partie relative aux règles de sécurité applicables. Elle constitue donc une traduction concrète de la stratégie de sécurité de l'organisme.

Quoique puisse suggérer ce document, la politique de sécurité en vigueur dans votre service doit primer.

Cette section précise néanmoins quelques mesures générales de nature à vous prémunir contre les agressions décrites dans ce document. En effet, la sécurité des systèmes d'information ne repose pas exclusivement sur des outils, mais aussi sur une organisation et des politiques.

10.2 Concevoir une architecture robuste

A la lumière des enseignements tirés de ce qui a été présenté dans les bulletins d'actualité, il convient de vérifier que les applications mises en oeuvre (ou à l'étude) ont une architecture qui résiste aux incidents décrits.

10.3 Appliquer les correctifs de sécurité

Le tableau 2 rappelle les avis du CERTA correspondant aux applications ou codes malveillants relatifs aux ports étudiés dans les sections précédentes.

10.4 Utiliser un pare-feu

L'application des correctifs sur un parc informatique important n'est probablement pas immédiate. Un pare-feu correctement configuré peut retenir certaines attaques informatiques le temps d'appliquer les correctifs. Cependant un pare-feu peut donner une illusion de protection. Cette protection est brisée par la moindre introduction d'un ordinateur nomade dans la partie protégée. On remarque qu'il y a de nombreux paquets rejetés à destination de ports légitimement utilisés par des applications de prise de main à distance. La téléadministration correspond à une demande qui grandit avec la taille du parc à gérer. Les paquets rejetés montrent le risque associé à ce type d'application. Ce risque peut être amoindri par l'usage correct d'un pare-feu.

10.5 Analyser le réseau

De nombreux paquets rejetés étudiés correspondent aux ports ouverts par divers virus/vers/chevaux de Troie. Si votre politique de sécurité autorise le balayage des ports ouverts sur les postes de travail ou les serveurs, il peut s'avérer utile de le faire régulièrement afin de découvrir les machines potentiellement contaminées avant qu'un intrus ne le fasse à votre place.

L'analyse des journaux de votre pare-feu est une source pertinente d'informations pour la sécurité de votre réseau et de vos systèmes. Cela peut vous aider à anticiper des incidents en remarquant par exemple des activités anormales. Le CERTA peut vous aider dans ce travail d'analyse.

10.6 Réagir aux incidents de sécurité

Organisez-vous pour réagir aux incidents de sécurité, en particulier, pour assurer une certaine continuité dans les équipes d'administration et de sécurité.

Le CERTA a pour mission de vous aider à répondre aux incidents de sécurité informatique.

Ne traitez pas les dysfonctionnements des machines à la légère. Dans certains incidents dans lesquels le CERTA intervient, les administrateurs des machines font spontanément part de petits dysfonctionnements inexplicables et d'apparence anodine qui s'avèrent, au cours de l'analyse, être liés à un incident majeur de sécurité. N'hésitez pas à prendre contact avec le CERTA si vous constatez de l'activité sur les ports décrits ci-dessus.

10.7 Former et sensibiliser les utilisateurs

La sécurité d'un système d'information doit reposer sur une approche de défense en profondeur. Cela signifie, entre autres choses, que l'utilisateur est partie prenante de la sécurité. Sa vigilance, son niveau de formation et de sensibilisation participent à la sécurité du système. C'est pourquoi il est essentiel de prévoir des séances de formation et de sensibilisation des utilisateurs, acteurs de la sécurité. Pour vous aider dans ces actions, la DCSSI dispose d'un centre de formation :

<http://www.formation.ssi.gouv.fr>

11 Les bulletins d'actualité

L'objectif des *bulletins d'actualité* est de fournir une illustration par l'actualité récente de certaines mesures de sécurité pragmatiques à appliquer. Bien que par nature *a posteriori*, cette illustration a vocation à servir de base pour tirer des enseignements plus généraux à même de protéger contre des incidents futurs.

L'« actualité » est donnée par l'analyse de machines que le CERTA réalise dans le cadre de ses missions. Un fait est jugé d'actualité, s'il est à la fois récent et significatif, c'est à dire recoupé par différentes analyses.

Les *bulletins d'actualité* n'ont pas la prétention de constituer des statistiques fiables de l'activité informatique malveillante, mais ce qui nous semble avoir beaucoup plus d'intérêt, de montrer à partir d'exemples concrets, réels et anonymisés comment découvrir que l'on est ou a été attaqué et comment limiter l'impact de ces attaques.

La qualité des *bulletins d'actualité* sera améliorée grâce à votre participation. Si vous souhaitez participer, prenez contact avec le CERTA en accord avec votre chaîne fonctionnelle de la sécurité des systèmes d'information.

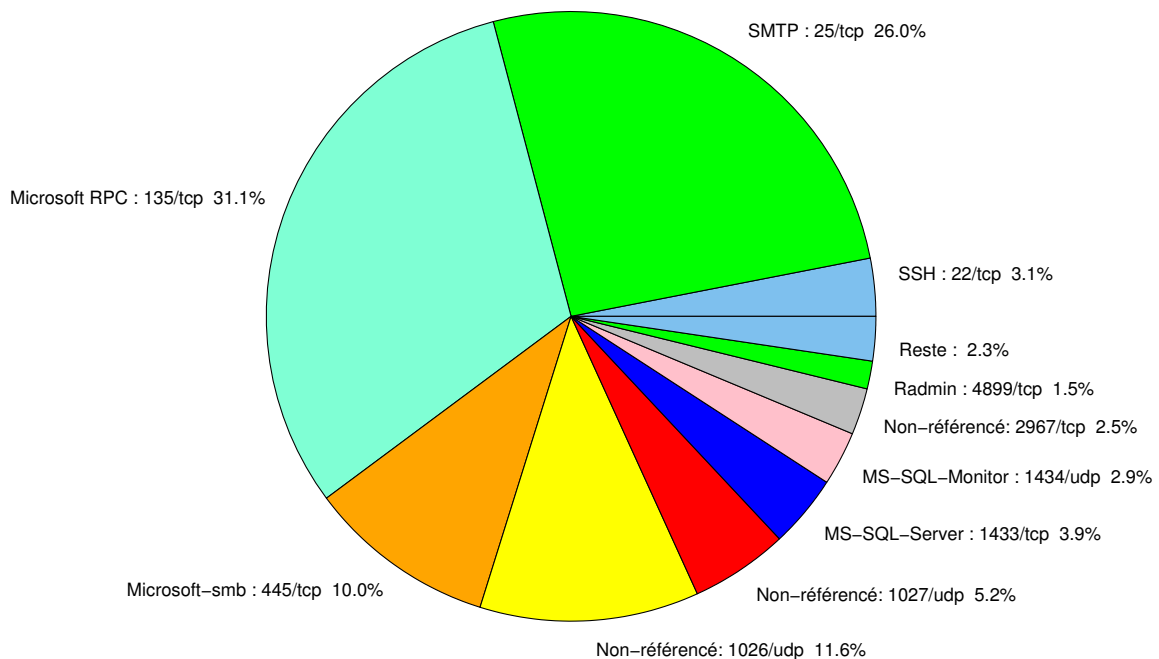


FIG. 1: Répartition relative des ports pour la semaine du 02.10.2008 au 09.10.2008

Port	Protocole	Service	Porte dérobée	Référence possible CERTA
21	TCP	FTP	–	CERTA-2003-AVI-132 CERTA-2004-AVI-064 CERTA-2004-AVI-066 CERTA-2006-AVI-040
22	TCP	SSH	–	CERTA-2003-AVI-152 CERTA-2006-AVI-100
23	TCP	Telnet	–	CERTA-2003-AVI-209 CERTA-2003-AVI-131 CERTA-2007-ALE-005-001
25	TCP	SMTP	–	CERTA-2006-AVI-124 CERTA-2006-AVI-135
42	TCP	WINS	–	CERTA-2004-AVI-384
69	UDP	IBM Tivoli Provisioning Manager	–	CERTA-2007-AVI-320
80	TCP	HTTP	–	CERTA-2004-AVI-195 CERTA-2004-AVI-239 CERTA-2006-AVI-055 CERTA-2006-AVI-069 CERTA-2006-AVI-156 CERTA-2006-AVI-315
106	TCP	MailSite Email Server	–	– CERTA-2007-AVI-008
111	TCP	Sunrpc-portmapper	–	CERTA-2003-AVI-052
119	TCP	NNTP	–	CERTA-2004-AVI-340
135	TCP	Microsoft RPC	–	CERTA-2003-ALE-002 CERTA-2003-AVI-111 CERTA-2004-AVI-127
137	UDP	NetBios-ns	–	CERTA-2004-AVI-031
139	TCP	NetBios-ssn et samba	–	CERTA-2004-AVI-368 CERTA-2003-AVI-168 CERTA-2004-AVI-126 CERTA-2005-AVI-051 CERTA-2005-AVI-213 CERTA-2005-AVI-302 CERTA-2005-AVI-398 CERTA-2006-AVI-283 CERTA-2006-AVI-338 CERTA-2007-AVI-321
143	TCP	IMAP	–	CERTA-2005-AVI-185
389	TCP	LDAP	–	CERTA-2003-AVI-102 CERTA-2003-AVI-068 CERTA-2003-AVI-041 CERTA-2003-AVI-004 CERTA-2004-AVI-126 CERTA-2007-AVI-294
427	TCP	Novell Client	–	CERTA-2006-AVI-538
443	TCP	HTTPS	–	CERTA-2003-AVI-156 CERTA-2004-AVI-126 CERTA-2004-AVI-247 CERTA-2004-AVI-343 CERTA-2007-AVI-153
445	TCP	Microsoft-smb	–	CERTA-2004-AVI-053 CERTA-2003-AVI-105 CERTA-2004-AVI-126 CERTA-2005-AVI-051 CERTA-2005-AVI-302 CERTA-2006-AVI-283

				CERTA-2006-AVI-338 CERTA-2007-AVI-321 CERTA-2007-ALE-010
445	UDP	Microsoft-smb	–	CERTA-2007-ALE-010
1023	TCP	–	Serveur ftp de Sasser.E	–
1080	TCP	Wingate	MyDoom.F	CERTA-2006-AVI-232
1433	TCP	MS-SQL-Server	–	CERTA-2002-ALE-006
1434	UDP	MS-SQL-Monitor	–	CERTA-2002-AVI-157
2100	TCP	Oracle XDB FTP	–	CERTA-2005-ALE-002
2381	TCP	HP System Management	–	CERTA-2006-AVI-248
2512	TCP	Citrix MetaFrame	–	CERTA-2006-AVI-491
2513	TCP	Citrix MetaFrame	–	CERTA-2006-AVI-491
2745	TCP	–	Bagle	–
2967	TCP	Symantec Antivirus	Yellow Worm	CERTA-2006-AVI-221
3104	TCP	CA Message Queuing	–	CERTA-2007-AVI-331
3127	TCP	–	MyDoom	–
3128	TCP	Squid	MyDoom	CERTA-2004-AVI-062 CERTA-2004-AVI-186 CERTA-2004-AVI-316 CERTA-2004-AVI-348
3268	TCP	Microsoft Active Directory	–	CERTA-2007-AVI-294
3306	TCP	MySQL	–	–
4899	TCP	Radmin	–	–
5000	TCP	Universal Plug and Play	Bobax, Kibuv	CERTA-2001-AVI-165 CERTA-2006-AVI-212 CERTA-2006-AVI-297
5151	UDP	IPSwitch WS_TP	–	CERTA-2007-AVI-312
5151	TCP	ESRI ArcSDE	–	CERTA-2007-AVI-367
5554	TCP	SGI ESP HTTP	Serveur ftp de Sasser	–
5900	TCP	VNC	–	CERTA-2006-AVI-198 CERTA-2006-AVI-299
6014	TCP	IBM Tivoli Monitoring	–	CERTA-2007-AVI-183
6070	TCP	BrightStor ARCserve/Enterprise Backup	–	CERTA-2005-AVI-293
6101	TCP	Veritas Backup Exec	–	CERTA-2005-AVI-024
6106	TCP	Symantec Backup Exec	–	CERTA-2007-AVI-303
6129	TCP	Dameware Miniremote	–	CERTA-2003-AVI-214 CERTA-2005-AVI-326
6502	TCP	CA BrightStor ARCserve Backup	–	CERTA-2007-AVI-029
6503	TCP	CA BrightStor ARCserve Backup	–	CERTA-2007-AVI-029
6504	TCP	CA BrightStor ARCserve Backup	–	CERTA-2007-AVI-029
8080	TCP	IBM Tivoli Provisioning Manager	–	CERTA-2007-AVI-153
8866	TCP	–	Porte dérobée Bagle.B	–
9898	TCP	–	Porte dérobée Dabber	–
10000	TCP	Webmin, Veritas Backup Exec	–	CERTA-2005-AVI-229 CERTA-2005-AVI-313
10080	TCP	Amanda	MyDoom	–
10110	TCP	IBM Tivoli Monitoring	–	CERTA-2007-AVI-183
10916	TCP	Ingres	–	CERTA-2007-AVI-275-001
10925	TCP	Ingres	–	CERTA-2007-AVI-275-001
12168	TCP	CA eTrust antivirus	–	CERTA-2007-AVI-217
13701	TCP	Veritas NetBackup	–	CERTA-2005-AVI-447
18264	TCP	CheckPoint interface	–	CERTA-2005-AVI-310
54345	TCP	HP Mercury	–	CERTA-2007-AVI-075
65535	UDP	LANDesk Management Suite	–	CERTA-2007-AVI-176

TAB. 2: Correctifs correspondant aux ports destination des paquets rejetés

port	pourcentage
135/tcp	31.06
25/tcp	26.04
1026/udp	11.62
445/tcp	9.99
1027/udp	5.17
1433/tcp	3.86
22/tcp	3.06
1434/udp	2.86
2967/tcp	2.46
4899/tcp	1.47
137/udp	0.55
23/tcp	0.43
80/tcp	0.31
3128/tcp	0.27
2100/tcp	0.15
143/tcp	0.07
1080/tcp	0.03

TAB. 3: Paquets rejetés

Liste des tableaux

1	Gestion du document	1
2	Correctifs correspondant aux ports destination des paquets rejetés	10
3	Paquets rejetés	11

Gestion détaillée du document

10 octobre 2008 version initiale.