



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité
des systèmes d'information
CERTA

Paris, le 10 août 2007
N° CERTA-2007-ACT-032

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2007-32

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-2007-ACT-032>

Gestion du document

Référence	CERTA-2007-ACT-032
Titre	Bulletin d'actualité 2007-32
Date de la première version	10 août 2007
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-2007-ACT-032.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-2007-ACT-032/>

1 Les méthodes d'attaques les plus simples sont efficaces

Si certaines intrusions reposent sur des techniques sophistiquées comme les débordements de tampons (*buffer overflow*) ou les insertions de code (ex. : *PHP-include*), les attaques contre les mots de passe faibles restent d'actualité. Un incident récemment traité par le CERTA l'a encore prouvé.

Une attaque par recherche exhaustive, c'est-à-dire en essayant toutes les combinaisons possibles, suffit à trouver le mot de passe, d'autant plus facilement qu'il est court ou simple. L'absence de blocage du compte après un certain nombre d'échecs permet de mener à terme une telle attaque.

Pour se prémunir de cette faiblesse, il convient d'adopter une politique de gestion stricte des mots de passe et des échecs d'authentification.

En complément, une conservation de la trace des échecs de connexion et une analyse régulière des journaux permet de détecter des attaques par dictionnaire ou par recherche exhaustive. Cette détection peut avoir lieu avant que la découverte du mot de passe n'aboutisse ou avant l'exploitation de la découverte du mot de passe.

Documentation

Note d'information du CERTA CERTA-2005-INF-001 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-001>

2 Attaques indirectes et dissimulation

Dans le bulletin d'actualité CERTA-2007-ACT-025, le CERTA présentait les cadres incorporés dans les pages HTML à l'aide de la balise `<IFRAME>`. Une utilisation frauduleuse est l'insertion d'un tel cadre pour diriger, de manière invisible, l'internaute qui visite un site légitime vers un site peu recommandable, par exemple hébergeant des logiciels malveillants qui vont tenter de s'installer sur le poste de cet internaute.

La politique d'un organisme, en matière de développement des sites, peut exclure l'utilisation de ces cadres. Un processus automatique peut vérifier constamment la présence de la balise `<IFRAME>` et son bien-fondé.

Une technique utilisable par les intrus qui insèrent ces cadres de manière malveillante consiste à ajouter, non pas le cadre lui-même, mais un script qui « déchiffre » un `javascript` représenté par un chaîne d'apparence aléatoire. Ce `javascript` écrit alors le fragment de code HTML qui construit le cadre malveillant. 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, très à droite pour ne pas être visible sur un écran de largeur ordinaire ;
- une connexion inattendue lors de la consultation du site légitime.

La technique qui transforme le script en chaîne de caractères d'apparence aléatoire est assez simple. Elle permet de créer une multitude de variantes pour un même script. De ce fait, un script identique aura autant d'apparences différentes qu'il y aura de pages modifiées de manière frauduleuse sur un même site. Cette variété freine la détection ciblée de ce script.

Aux recommandations du bulletin d'actualité précité, le CERTA ajoute :

- la désactivation de l'exécution systématique des scripts dans les navigateurs ;
- l'affichage de la barre d'état dans le navigateur et la surveillance de celle-ci. Il faut être vigilant si, lors de la visite d'un site, une connexion vers un site tiers se déclenche.

Les développeurs de sites web peuvent en déduire que l'usage des scripts sur leurs sites est un frein à la protection de l'internaute.

Comme des sites proposent des versions « texte seul », « sans cadre » ou « sans frames », des versions dans diverses langues, des alternatives « HTML ou flash », ils peuvent proposer des versions « sans scripts ».

Documentation

Bulletin d'actualité du CERTA CERTA-2007-ACT-025 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2007-ACT-025/>

3 Une trace anodine dans les journaux des connexions

Cette semaine le CERTA a mis en évidence et traité deux compromissions grâce aux journaux des connexions. La première compromission est un exemple de la coopération et des liens internationaux existant entre les CSIRTs (les équipes homologues à celle du CERTA). Lors de l'analyse des journaux des connexions d'un serveur web, le CERTA a relevé une tentative, infructueuse, d'intrusion. Cette tentative provenait en fait d'une machine connectée sur un réseau universitaire à l'étranger. Le CERTA a immédiatement prévenu ses contacts privilégiés dans ce pays. Cette information leur a permis de mettre en évidence une machine compromise faisant partie d'un réseau de machines zombies (*Botnet*).

La seconde compromission a été mise en évidence par la trace, dans un journal des connexions, d'un comportement suspect. Une machine tentait périodiquement de télécharger une application sur un serveur situé à l'étranger. Un tel comportement a attiré l'attention d'autant plus que l'application en question était un virus. L'analyse en cours de cette compromission montre que cette machine, bien que possédant un logiciel antivirus à jour, est hautement compromise par une multitude de virus et autres logiciels malveillants.

Le CERTA rappelle que les journaux des connexions doivent être analysés et surveillés régulièrement. Un comportement inhabituel qui peut paraître anodin doit être relevé afin de mettre en évidence une compromission, une tentative d'attaque ponctuelle ou une attaque étalée dans le temps.

Documentation

Note d'information du CERTA CERTA-2002-INF-002 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2002-INF-002/>

4 Ports observés

Le tableau 3 et la figure 1 montrent les rejets pour les ports sous surveillance que nous avons constatés sur deux dispositifs de filtrage, entre le 02 août et le 09 août 2007.

5 Liens utiles

- Mémento du CERTA 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 du CERTA 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/>

6 Rappel des avis émis

Durant la période du 02 août au 09 août 2007, le CERTA a émis les avis suivants :

- CERTA-2007-AVI-344 : Vulnérabilité de Kaspersky Antispam
- CERTA-2007-AVI-345 : Vulnérabilité de Tomcat
- CERTA-2007-AVI-346 : Vulnérabilité de Java System Web Server
- CERTA-2007-AVI-347 : Multiples vulnérabilités dans HP System Management Homepage
- CERTA-2007-AVI-349 : Vulnérabilité dans la machine virtuelle Java de Sun

Pendant la même période, l'avis suivant a été mis à jour :

- CERTA-2007-AVI-226-002 : Vulnérabilité dans FreeType (ajout des références aux bulletins de sécurité des éditeurs)
- CERTA-2007-AVI-313-001 : Vulnérabilité dans la bibliothèque libarchive (modification des systèmes affectés, ajout des références CVE et des références aux bulletins de sécurité Gentoo et SuSE)
- CERTA-2007-AVI-348-001 : Multiples vulnérabilités dans la machine Java d'IBM (modification des systèmes affectés, ajout des références CVE et des bulletins de sécurité des éditeurs SuSE, Red Hat, Avaya et Gentoo)

7 Actions suggérées

7.1 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.

7.2 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 œuvre (ou à l'étude) ont une architecture qui résiste aux incidents décrits.

7.3 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.

7.4 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.

7.5 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 COSSI/CERTA peut vous aider dans ce travail d'analyse.

7.6 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.

7.7 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>

8 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.

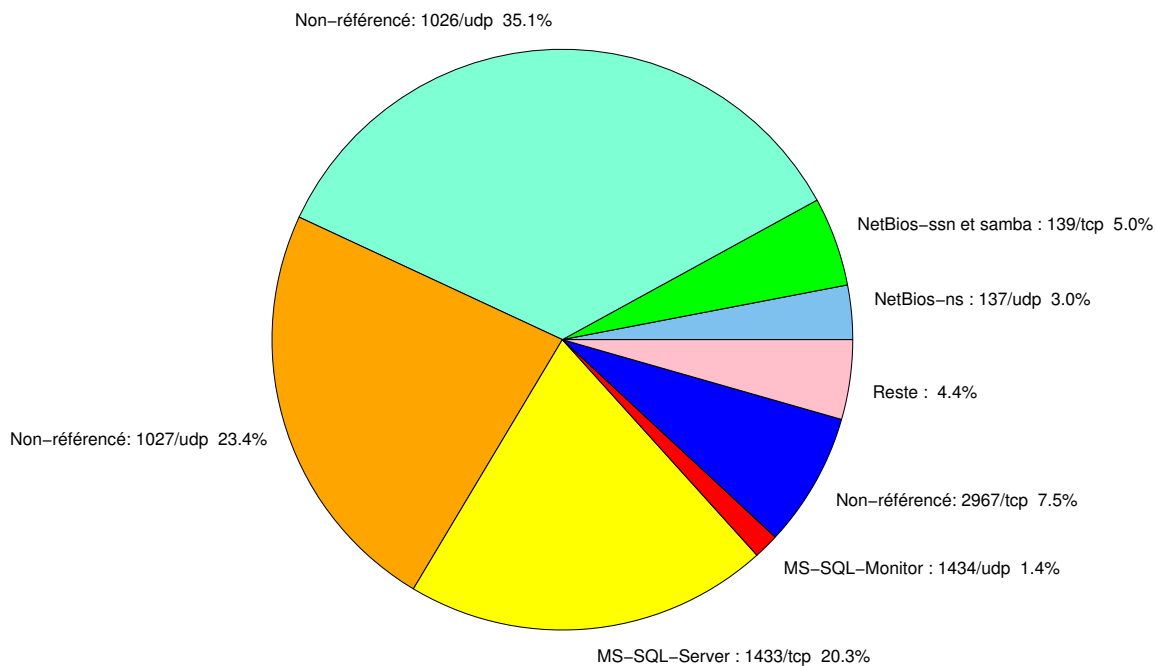


FIG. 1: Répartition relative des ports pour la semaine du 02.08.2007 au 09.08.2007

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
25	TCP	SMTP	-	CERTA-2006-AVI-124 CERTA-2006-AVI-135
42	TCP	WINS	-	CERTA-2004-AVI-384
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	-	-
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
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
443	TCP	HTTPS	-	CERTA-2003-AVI-156 CERTA-2004-AVI-126 CERTA-2004-AVI-247 CERTA-2004-AVI-343
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
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
2745	TCP	–	Bagle	–
2967	TCP	Symantec Antivirus	Yellow Worm	CERTA-2006-AVI-221
3127	TCP	–	MyDoom	–
3128	TCP	Squid	MyDoom	CERTA-2004-AVI-062 CERTA-2004-AVI-186 CERTA-2004-AVI-316 CERTA-2004-AVI-348
3306	TCP	MySQL	–	–
3389	TCP	Microsoft RDP	–	CERTA-2002-AVI-213
4899	TCP	Radmin	–	–
5000	TCP	Universal Plug and Play	Bobax, Kibuv	CERTA-2001-AVI-165 CERTA-2006-AVI-212 CERTA-2006-AVI-297
5554	TCP	SGI ESP HTTP	Serveur ftp de Sasser	–
5900	TCP	VNC	–	CERTA-2006-AVI-198 CERTA-2006-AVI-299
6070	TCP	BrightStor ARCserve/Enterprise Backup	–	CERTA-2005-AVI-293
6101	TCP	Veritas Backup Exec	–	CERTA-2005-AVI-024
6112	TCP	Dtspcd	–	CERTA-2002-ALE-001
6129	TCP	Dameware Miniremote	–	CERTA-2003-AVI-214 CERTA-2005-AVI-326
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	–
13701	TCP	Veritas NetBackup	–	CERTA-2005-AVI-447
18264	TCP	CheckPoint interface	–	CERTA-2005-AVI-310

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

port	pourcentage
1026/udp	35.09
1027/udp	23.35
1433/tcp	20.25
2967/tcp	7.46
139/tcp	4.95
137/udp	3.01
1434/udp	1.41
22/tcp	0.75
1080/tcp	0.61
3128/tcp	0.54
80/tcp	0.48
4899/tcp	0.46
3306/tcp	0.31
23/tcp	0.27
25/tcp	0.23
21/tcp	0.21
143/tcp	0.16
3389/tcp	0.12
9898/tcp	0.1
5554/tcp	0.08
1023/tcp	0.02

TAB. 3: Paquets rejetés

Liste des tableaux

1	Gestion du document	1
2	Correctifs correspondant aux ports destination des paquets rejetés	7
3	Paquets rejetés	8

Gestion détaillée du document

10 août 2007 version initiale.