

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2010-27

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-2010-ACT-027>

Gestion du document

Référence	CERTA-2010-ACT-027
Titre	Bulletin d'actualité 2010-27
Date de la première version	09 juillet 2010
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-2010-ACT-027.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-2010-ACT-027/>

1 De l'utilité des dates dans l'historique du shell

Cette semaine, le CERTA a traité un incident ayant eu lieu sur un serveur Linux. L'analyse des traces a été grandement facilitée par un élément de configuration du serveur qui permet d'associer une date à chaque action de l'historique du *shell*. L'administrateur avait mis en place la variable d'environnement HISTTIMEFORMAT de l'interpréteur de commandes *bash*.

Le CERTA a donc pu tracer beaucoup plus facilement les actions réalisées par l'intrus sur le système.

Le CERTA recommande de mettre en place cette option à l'installation du système. C'est une mesure qui peut se révéler inestimable pour savoir ce qu'il s'est passé, notamment en cas de problème de sécurité sur la machine.

2 Vulnérabilité dans Ubuntu

Cette semaine, le CERTA a publié l'avis CERTA-2010-AVI-304 relatif à une vulnérabilité spécifique à la version d'un module PAM (*Pluggable Authentication Modules*) présent dans les versions 9.10 et 10.04 de la distribution GNU/Linux Ubuntu. Cette vulnérabilité permet à un utilisateur disposant d'un compte sur le système vulnérable d'élever ses privilèges.

Le côté inhabituel de cette faille réside dans le fait qu'elle ne nécessite pas d'outils spécifiques exploitant tel pointeur nul ou tel autre débordement de mémoire. L'attaquant a uniquement et simplement à profiter d'un manque de contrôles de la part d'un module PAM lui permettant de façon triviale de passer administrateur de la machine. Il lui suffit de disposer d'un accès quelconque sur le système (par exemple local, ou encore via SSH ou telnet), l'exploitation se faisant à la connexion.

En outre, il est à noter que, au niveau des journaux système, la seule trace sera une authentification réussie de la part d'un utilisateur légitime !

Le CERTA invite donc fortement les utilisateurs des versions Ubuntu 9.10 et 10.04 à mettre à jour leur système dans les plus brefs délais en appliquant le correctif décrit dans le bulletin de sécurité USN-959-1.

Documentation :

- Avis CERTA-2010-AVI-304 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2010-AVI-304/>

3 Annonce d'un réseau de smartphones zombies

Un article, largement relayé sur l'Internet, annonce la découverte d'un réseau de 100 000 *smartphones* zombies. L'origine de cette annonce étant une société commercialisant une solution antivirus pour téléphones mobiles, sa véracité, ou tout du moins son ampleur, sont à prendre avec du recul. Selon la description faite du logiciel, le code se propagerait en envoyant des SMS contenant une adresse pointant sur un programme malveillant au nom attrayant et d'actualité, et cela à tous les contacts du répertoire et à d'autres numéros aléatoires. Il semble donc que l'infection du terminal mobile nécessite une action de la part de la victime.

Si cette annonce semble un peu trop orientée pour être complètement crédible, le risque d'infection des terminaux mobiles est réel. Il s'agit de machines autonomes connectées, communicantes et rarement mises à jour. Ces *SmartPhones* contiennent de plus en plus fréquemment des documents de travail et autres informations sensibles. Ils peuvent même être utilisés comme micro d'ambiance. Ils sont encore à la frontière du personnel et du professionnel et n'apparaissent pas souvent dans les PSSI malgré les risques qu'ils entraînent. Les risques qu'ils soient touchés et que cela ait un impact sur la sécurité locale sont bien réels et ne doivent donc pas être ignorés.

Encore une fois, le CERTA recommande pour l'utilisation de ces terminaux mobiles d'appliquer les mêmes bonnes pratiques que pour un ordinateur portable classique. À savoir, entre autres :

- appliquer les correctifs de sécurité ;
- maîtriser les informations stockées dessus ;
- ne pas accepter de documents (par messagerie électronique, SMS, Bluetooth, ...) non attendus ;
- n'activer les interfaces de communication qu'au besoin (WiFi, Bluetooth, ...) ;
- ne pas le laisser sans surveillance ;
- vérifier les journaux locaux (appels, SMS, ...) et les factures ;
- et surtout en avoir une utilisation réfléchie et conforme avec la PSSI.

4 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=1937>
- 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/>

5 Rappel des avis émis

Dans la période du 02 au 08 juillet 2010, le CERTA a émis les avis suivants :

- CERTA-2010-AVI-299 : Vulnérabilité de sudo
- CERTA-2010-AVI-300 : Multiples vulnérabilités dans Google Chrome
- CERTA-2010-AVI-301 : Vulnérabilité dans Bogofilter
- CERTA-2010-AVI-302 : Multiples vulnérabilités dans Novell Identity Manager
- CERTA-2010-AVI-303 : Vulnérabilité dans les commutateurs Cisco Industrial Ethernet 3000 series
- CERTA-2010-AVI-304 : Vulnérabilité dans Ubuntu
- CERTA-2010-AVI-305 : Vulnérabilité dans Ruby

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

- CERTA-2010-AVI-260-002 : Vulnérabilités dans Wireshark (ajout des références aux bulletins de sécurité Mandriva et Debian)
- CERTA-2010-AVI-295-001 : Vulnérabilité dans Citrix XenServer (ajout de la référence CVE)
- CERTA-2010-AVI-297-001 : Vulnérabilités sur OpenVMS (ajout de la référence CVE)

6 Actions suggérées

6.1 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.

6.2 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.

6.3 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.

6.4 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.

6.5 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.

6.6 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.

6.7 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, l'ANSSI dispose d'un centre de formation :

http://www.ssi.gouv.fr/site_rubrique67.html

7 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.

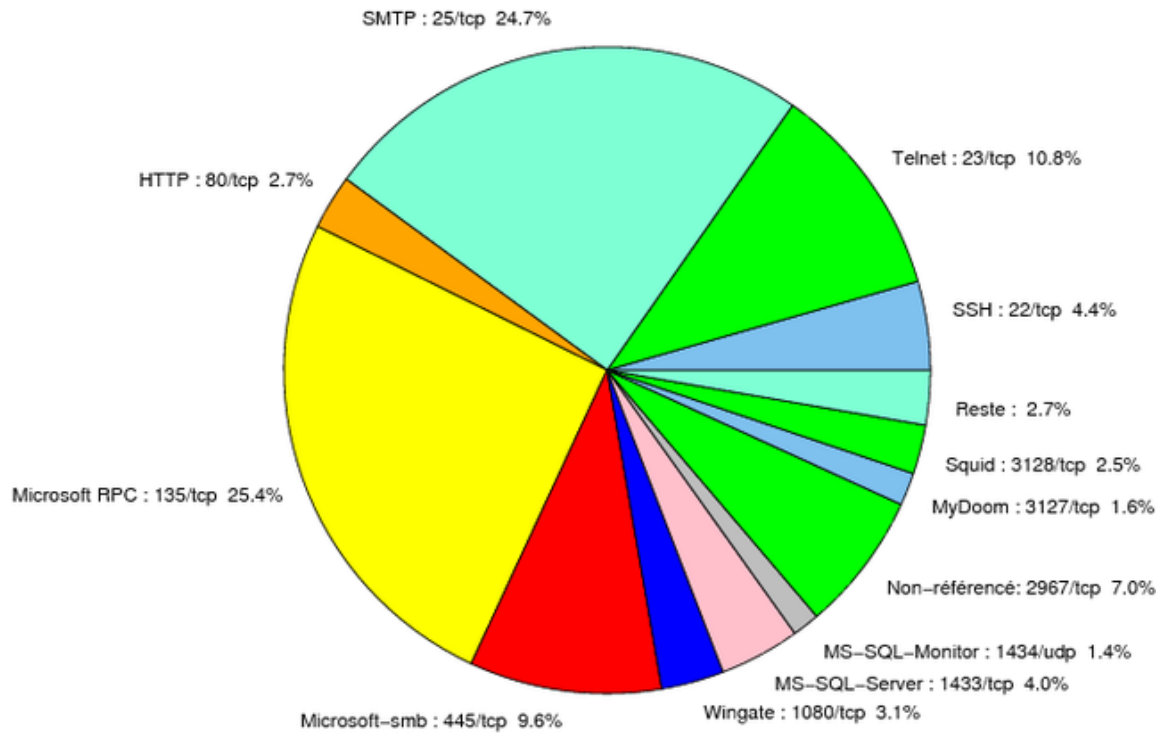


FIG. 1: Répartition relative des ports pour la semaine du 02 au 08 juillet 2010

Port	Protocole	Service	Porte dérobée	Référence possible CERTA
21	TCP	FTP	-	http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001
22	TCP	SSH	-	http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001
23	TCP	Telnet	-	http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001
25	TCP	SMTP	-	http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001
42	TCP	WINS	-	http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001
69	UDP	IBM Tivoli Provisioning Manager	-	http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001
80	TCP	HTTP	-	http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001
106	TCP	MailSite Email Server	-	http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001
111	TCP	Sunrpc-portmapper	-	http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001
119	TCP	NNTP	-	http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001
135	TCP	Microsoft RPC	-	http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001
137	UDP	NetBios-ns	-	http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001
139	TCP	NetBios-ssn et samba	-	http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001

				http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
143	TCP	IMAP	–	http://www.certa.ssi.gouv.fr/site/CER
389	TCP	LDAP	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
427	TCP	Novell Client	–	http://www.certa.ssi.gouv.fr/site/CER
443	TCP	HTTPS	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
445	TCP	Microsoft-smb	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
445	UDP	Microsoft-smb	–	http://www.certa.ssi.gouv.fr/site/CER
1023	TCP	–	Serveur ftp de Sasser.E	–
1080	TCP	Wingate	MyDoom.F	http://www.certa.ssi.gouv.fr/site/CER
1433	TCP	MS-SQL-Server	–	http://www.certa.ssi.gouv.fr/site/CER
1434	UDP	MS-SQL-Monitor	–	http://www.certa.ssi.gouv.fr/site/CER
2100	TCP	Oracle XDB FTP	–	http://www.certa.ssi.gouv.fr/site/CER
2381	TCP	HP System Management	–	http://www.certa.ssi.gouv.fr/site/CER
2512	TCP	Citrix MetaFrame	–	http://www.certa.ssi.gouv.fr/site/CER
2513	TCP	Citrix MetaFrame	–	http://www.certa.ssi.gouv.fr/site/CER
2745	TCP	–	Bagle	–
2967	TCP	Symantec Antivirus	Yellow Worm	http://www.certa.ssi.gouv.fr/site/CER
3104	TCP	CA Message Queuing	–	http://www.certa.ssi.gouv.fr/site/CER
3127	TCP	–	MyDoom	–
3128	TCP	Squid	MyDoom	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
3268	TCP	Microsoft Active Directory	–	http://www.certa.ssi.gouv.fr/site/CER
3306	TCP	MySQL	–	–
4899	TCP	Radmin	–	–
5000	TCP	Universal Plug and Play	Bobax, Kibuv	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
5151	UDP	IPSwitch WS_TP	–	http://www.certa.ssi.gouv.fr/site/CER
5151	TCP	ESRI ArcSDE	–	http://www.certa.ssi.gouv.fr/site/CER
5554	TCP	SGI ESP HTTP	Serveur ftp de Sasser	–
5900	TCP	VNC	–	http://www.certa.ssi.gouv.fr/site/CER

				http://www.certa.ssi.gouv.fr/site/CER
6014	TCP	IBM Tivoli Monitoring	-	http://www.certa.ssi.gouv.fr/site/CER
6070	TCP	BrightStor ARCserve/Enterprise Backup	-	http://www.certa.ssi.gouv.fr/site/CER
6101	TCP	Veritas Backup Exec	-	http://www.certa.ssi.gouv.fr/site/CER
6106	TCP	Symantec Backup Exec	-	http://www.certa.ssi.gouv.fr/site/CER
6129	TCP	Dameware Miniremote	-	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
6502	TCP	CA BrightStor ARCserve Backup	-	http://www.certa.ssi.gouv.fr/site/CER
6503	TCP	CA BrightStor ARCserve Backup	-	http://www.certa.ssi.gouv.fr/site/CER
6504	TCP	CA BrightStor ARCserve Backup	-	http://www.certa.ssi.gouv.fr/site/CER
8080	TCP	IBM Tivoli Provisioning Manager	-	http://www.certa.ssi.gouv.fr/site/CER
8866	TCP	-	Porte dérobée Bagle.B	-
9898	TCP	-	Porte dérobée Dabber	-
10000	TCP	Webmin, Veritas Backup Exec	-	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
10080	TCP	Amanda	MyDoom	-
10110	TCP	IBM Tivoli Monitoring	-	http://www.certa.ssi.gouv.fr/site/CER
10916	TCP	Ingres	-	CERTA-2007-AVI-275-001
10925	TCP	Ingres	-	CERTA-2007-AVI-275-001
12168	TCP	CA eTrust antivirus	-	http://www.certa.ssi.gouv.fr/site/CER
13701	TCP	Veritas NetBackup	-	http://www.certa.ssi.gouv.fr/site/CER
18264	TCP	CheckPoint interface	-	http://www.certa.ssi.gouv.fr/site/CER
54345	TCP	HP Mercury	-	http://www.certa.ssi.gouv.fr/site/CER
65535	UDP	LANDesk Management Suite	-	http://www.certa.ssi.gouv.fr/site/CER

TAB. 2: Correctifs correspondant aux ports destination des paquets re-
jetés

port	pourcentage
135/tcp	25.42
25/tcp	24.67
80/tcp	14.04
23/tcp	10.9
445/tcp	9.61
2967/tcp	6.95
22/tcp	4.43
1433/tcp	4.02
1080/tcp	3.13
3128/tcp	2.45
3127/tcp	1.63
1434/udp	1.36
3389/tcp	0.88
5000/tcp	0.54
10080/tcp	0.13

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

09 juillet 2010 version initiale.