

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2009-44

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-2009-ACT-044>

Gestion du document

Référence	CERTA-2009-ACT-044
Titre	Bulletin d'actualité 2009-44
Date de la première version	30 octobre 2009
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-2009-ACT-044.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-2009-ACT-044/>

1 Microsoft EMET

Cette semaine Microsoft a publié un outil nommé EMET pour (Enhanced Mitigation Evaluation Toolkit) disponible en téléchargement gratuit à cette adresse :

<http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=4a2346ac-b772-4d40-a750-9046542f343d>.

Cet outil, bien qu'en ligne de commande, reste très simple à utiliser. Il ne dispose pas, pour le moment, de programme d'installation mais la documentation fournie étant assez claire, on peut s'en affranchir aisément.

EMET propose de positionner, de façon indépendante sur les programmes binaires présents sur la machine, un certain nombre de protections limitant les effets des codes malveillants. Ainsi, parmi les protections proposées, on trouve :

- l'activation du *DEP* (*Data Execution Prevention*) par binaire. Cette protection empêche l'exécution de certaines régions d'un processus en marquant explicitement ces zones comme non-exécutables. Cette fonctionnalité était déjà présente dans Windows XP SP2 ainsi que les versions suivantes pour les binaires Microsoft, mais EMET permet d'affiner les réglages en permettant ce positionnement binaire par binaire ;

- un système de protection de la chaîne d'exceptions ou *SEH* (Structured Exception Handling) inclus dans chaque binaire. Ce mécanisme prévient la corruption de cette chaîne. En effet, il existe des moyen d'exécuter du code arbitraire si l'on arrive à corrompre cette structure ;
- un système de protection des erreurs issu d'un type pointeur nul (*NULL Pointer*) présents dans certains programmes. *EMET* préviendra donc des attaques de type *NULL Pointer* même si le binaire protégé présente ce type de faille ;
- une protection de la zone mémoire nommée « tas » qui sert aux mécanismes d'allocation dynamique de mémoire. Une attaque assez courante consistant à remplir le tas avec des données comprenant, entre autre, le code arbitraire à exécuter (*shellcode*), *EMET* l'empêchera ou, tout du moins, rendra plus difficile ce type d'attaque.

Concrètement, *EMET* gère la liste des applications qu'il protège. Son fonctionnement est binaire puisque si l'application figure dans cette liste elle disposera de l'ensemble des protections si elle n'y est pas, elle n'en aura aucune, sauf peut-être le *DEP* si il a été positionné globalement par ailleurs.

Cet outil devra tout de même être utilisé avec prudence et modération car, selon Microsoft et compte tenu des protections mises en place, il peut y avoir des effets de bord pour certaines applications. Celles-ci peuvent tout simplement cesser de fonctionner ou devenir instables. Néanmoins pour des applications sensibles et souvent sujettes à des attaques, *EMET* peut être d'un grand secours et le niveau de protection offert se révèle être très intéressant. De plus son utilisation en ligne de commande lui permet d'être inclus aisément dans des *scripts* de configuration.

2 Problèmes avec la mise à jour MS09-056

La mise à jour MS09-056 corrige deux vulnérabilités de la *CryptoAPI* de Microsoft Windows permettant d'usurper le certificat d'un site Web. Ce bulletin a fait l'objet de l'avis CERTA-2009-AVI-436.

Microsoft a mis à jour son bulletin de sécurité pour informer de problèmes éventuels pouvant être rencontrés avec certaines applications après installation de la mise à jour. Notamment, il est écrit que certains services ne s'exécutent plus dans les versions suivantes de Communications Server :

- Live Communications Server 2005 et Live Communications Server 2005 SP1 ;
- Office Communications Server 2007 Enterprise Edition, Standard Edition, et R2 Standard Edition ;
- les versions d'évaluation d'Office Communicator 2007 et Office Communicator R2.

Le symptôme décrit est que l'activation des produits échoue ou que les produits se comportent comme si une version d'évaluation expirée est installée.

Un correctif est disponible sur le site de Microsoft (cf. section documentation).

Documentation

- Article #974571 de la base de connaissances Microsoft :
<http://support.microsoft.com/kb/974571>
- Avis CERTA-2009-AVI-436 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2009-AVI-436/index.html>

3 Le numéro de téléphone : une illusion d'authentification

Ne jamais faire confiance à un service demandant une authentification par numéro de téléphone.

Si votre messagerie vocale n'est pas protégée par un mot de passe, il est judicieux d'en configurer un. Car il n'est pas forcément facile de savoir la façon dont l'opérateur gère l'authentification sur son serveur de messagerie.

Il est aujourd'hui possible de se faire passer pour un autre en usurpant son numéro de téléphone. L'avènement de la *VoIP* a mis le *spoofing* téléphonique, c'est-à-dire l'usurpation de numéro de téléphone, à la portée de tous. Avec un *PABX*, il est envisageable de manipuler les flux téléphoniques et donc de modifier le numéro source de l'appel.

N'importe qui peut alors usurper un numéro de téléphone. Il existe des services « légitimes » sur le Web agissant comme proxy téléphonique et permettant de changer le numéro source de l'appel, ainsi que de modifier sa voix. Ces services sont faciles à utiliser, il suffit d'y souscrire, pour environ 10 euros de l'heure, et un code *PIN* sera fourni qui permettra l'accès au proxy téléphonique. Ensuite, il suffit d'appeler ce proxy téléphonique, d'entrer le code *PIN*, et de préciser le numéro à appeler et le numéro source de l'appel. Certains *smartphones* peuvent installer directement des applications permettant d'automatiser ce processus.

Beaucoup de services, aux États-Unis notamment, utilisent le numéro de téléphone pour authentifier l'utilisateur. Des banques, des sociétés de vente par correspondance, des fournisseurs d'accès à l'Internet ou téléphonique, et bien d'autres encore, utilisent de nos jours l'authentification par numéro de téléphone. C'est malheureusement une donnée à laquelle les gens ont appris à faire confiance. Pourtant, cette forme d'authentification est aujourd'hui clairement obsolète. Il est beaucoup plus facile d'usurper un numéro de téléphone qu'il y a 10 ans.

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 23 au 29 octobre 2009, le CERTA a émis les avis suivants :

- CERTA-2009-AVI-454 : Multiples vulnérabilités dans TYPO3
- CERTA-2009-AVI-455 : Vulnérabilité dans IBM OS/400 HTTP Server
- CERTA-2009-AVI-456 : Vulnérabilité dans ProFTPD
- CERTA-2009-AVI-457 : Vulnérabilité dans Asterisk
- CERTA-2009-AVI-458 : Vulnérabilité dans IBM Lotus Connections
- CERTA-2009-AVI-459 : Multiples vulnérabilités dans Mozilla Firefox
- CERTA-2009-AVI-460 : Vulnérabilités dans Opera
- CERTA-2009-AVI-461 : Vulnérabilité dans Solaris Trusted Extensions
- CERTA-2009-AVI-462 : Vulnérabilités dans les produits McAfee
- CERTA-2009-AVI-463 : Multiples vulnérabilités dans Wireshark

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

- CERTA-2009-AVI-211-001 : Multiples vulnérabilités de Apache Tomcat (ajout de référence CVE et du bulletin HP-UX)

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_rubrique63.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.

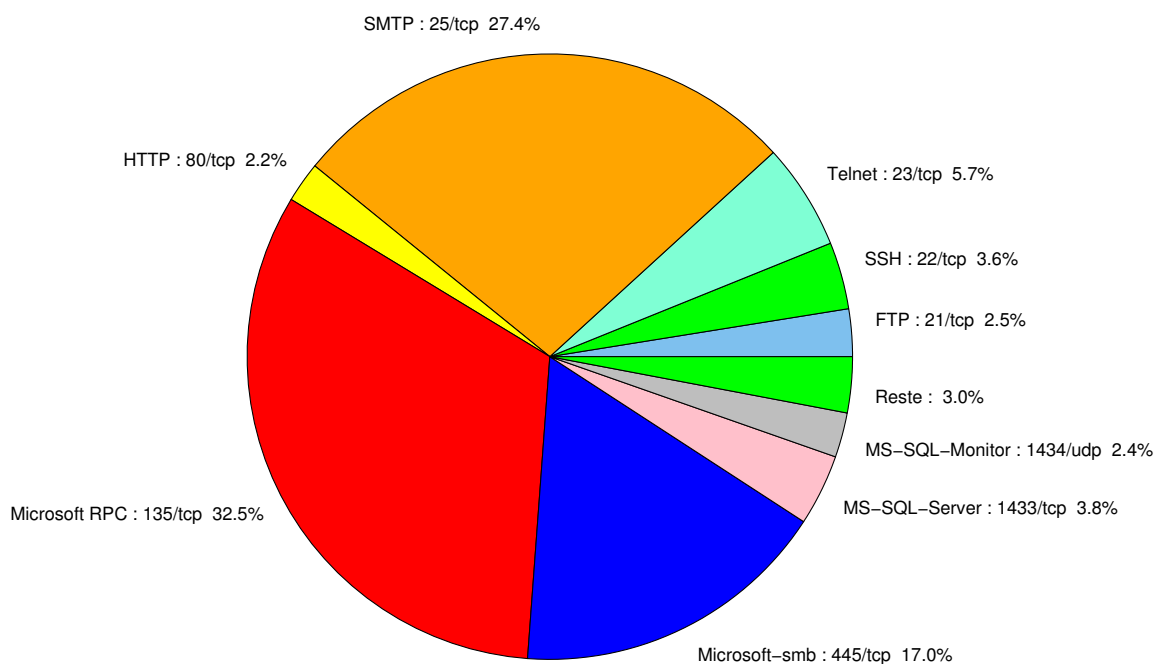


FIG. 1: Répartition relative des ports pour la semaine du 23 au 29 octobre 2009

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	32.51
25/tcp	27.36
445/tcp	17
23/tcp	5.66
1433/tcp	3.8
22/tcp	3.57
80/tcp	3.13
21/tcp	2.68
1434/udp	2.38
3128/tcp	0.89
2967/tcp	0.67
4899/tcp	0.44
1080/tcp	0.29
6101/tcp	0.14
3306/tcp	0.07

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

30 octobre 2009 version initiale.