Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 04 février 2011
N° CERTA-2011-ACT-005

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2011-05

Gestion du document

Référence	CERTA-2011-ACT-005
Titre	Bulletin d'actualité 2011-05
Date de la première version	04 février 2011
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-2011-ACT-005.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-2011-ACT-005/

1 Incident de la semaine

Rappel de bonnes pratiques

Dans le cadre d'un traitement d'incident, le CERTA a été amené à analyser une copie physique de la mémoire vive et du disque dur d'une machine. À l'analyse des deux copies, il apparaît que de nombreux utilitaires de détection de codes malveillants ont été lancés après la copie de la mémoire vive. Ces utilitaires ont malheureusement été exécutés par l'utilisateur lui-même qui les avait installés auparavant.

Le CERTA rappelle que ces utilitaires sont, au delà des aspects légaux, nuisibles à la conservation des certains éléments nécessaires à une analyse des traces et indices (date d'accès ou de modification, effacement de certains fichiers, ...). Le CERTA profite de cet événement pour rappeler certaines bonnes pratiques en matière de traitement d'incident :

- déconnecter la machine du réseau afin de stopper toute action malveillante depuis et vers l'Internet ;
- prévenir le responsable sécurité et/ou le CERT dont dépend votre entité ;
- effectuer une copie physique du disque ;
- rechercher les traces disponibles sur les équipements périphériques du réseau.

Documentation

– Note d'information CERTA-2002-INF-002-003 « Les bons réflexes en cas d'intrusion sur un système d'information » :
http://www.certa.ssi.gouv.fr/site/CERTA-2002-INF-003/

2 Vulnérabilité non corrigée dans Microsoft Windows

Microsoft a récemment publié un nouveau bulletin de sécurité (#2501696) concernant une faille non corrigée dans toutes les versions supportées de Microsoft Windows.

La vulnérabilité concerne l'interprétation de MHTML (*MIME HTML*) par Windows. Une personne malintentionnée peut ainsi, au moyen d'une page web spécialement conçue, exécuter du code *JavaScript* hors du contexte normalement permis. Il s'agit donc d'une vulnérabilité de type *cross-site scripting* ; après exploitation de la faille, l'attaquant peut ainsi accéder à des informations confidentielles provenant d'autres sites et effectuer des requêtes sur ces sites.

Cette vulnérabilité ne serait pas corrigée dans le lot des mises à jour du mois de février, selon Microsoft. En attendant l'éditeur a cependant mis en ligne un *fix-it* qui désactive l'interprétation du MHTML. Il est fortement recommandé d'appliquer ce contournement. La désactivation du *JavaScript* permet également de se prémunir de cette vulnérabilité.

Aucun cas d'exploitation n'a pour le moment été observé mais des preuves de faisabilité existent sur l'Internet.

Documentation

– Bulletin Microsoft #2501696 :
http://www.microsoft.com/technet/security/advisory/2501696.mspx
– « Fix-it » :
http://support.microsoft.com/kb/2501696

3 Compte de service et vulnérabilité

Cette semaine le CERTA a rencontré le cas d'un produit comportant une vulnérabilité liée au fait qu'un compte de service aux droits élevés était nécessaire au sein de ce logiciel pour réaliser certaines actions. Le problème réside dans le fait que, d'une part, ce compte utilisateur était utilisé par un des composants de l'application disposant de privilèges élevés sur le système et que, d'autre part, il était possible, par le biais de ce code, d'exécuter des commandes arbitraires à distance.

Nous sommes ici en présence d'une vulnérabilité induite par un problème de conception et de *design* et non pas due à une quelconque faille dans une des fonctions du logiciel. En effet, le problème est qu'un des composants accessibles à distance utilise un compte système particulier et privilégié pour réaliser un certain nombre d'opérations.

Une bonne pratique aurait consisté pour le développeur à mettre en œuvre, par exemple, une séparation de privilège du type : celui qui reçoit les commandes et les requêtes n'est pas celui qui les exécute. Ainsi même si un compte système est indispensable dans une partie du logiciel, cette dernière ne sera pas accessible à distance. Elle sera protégée, par exemple, par mécanisme d'`API` (`Application Programming Interface`) restreignant au maximum les actions dangereuses possibles. Dans une démarche de défense en profondeur, le mieux est de faire en sorte :

– que le niveau de privilège nécessaire au compte de service soit le plus bas possible ;
– que le composant s'appuyant sur ce compte ne soit pas appelable directement à distance mais uniquement localement et via une `API` ;
– que ce soit un autre composant qui face l'interface avec l'extérieur ; celui-ci jouant alors le rôle de mandataire.

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 28 janvier au 03 février 2011, le CERTA a émis les avis suivants :

– CERTA-2011-AVI-040 : Vulnérabilité dans RealPlayer
– CERTA-2011-AVI-041 : Vulnérabilité dans le serveur DHCPv6 d'ISC
– CERTA-2011-AVI-042 : Vulnérabilités dans IBM DB2
– CERTA-2011-AVI-043 : Vulnérabilités dans IBM Tivoli
– CERTA-2011-AVI-044 : Vulnérabilité dans le paquet exim4
– CERTA-2011-AVI-045 : Vulnérabilité dans Symantec IM Manager
– CERTA-2011-AVI-046 : Vulnérabilité dans VLC Media Player
– CERTA-2011-AVI-047 : Multiples vulnérabilités dans Apache CouchDB
– CERTA-2011-AVI-048 : Vulnérabilité dans EMC NetWorker
– CERTA-2011-AVI-049 : Vulnérabilité dans PMB
– CERTA-2011-AVI-050 : Multiples vulnérabilités dans Cisco WebEx Player

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

– CERTA-2010-AVI-465-001 : Vulnérabilité dans IBM DB2 Administration Server (ajout du bulletin IBM concernant les versions 91, 9.5 et 9.7.)
– CERTA-2011-AVI-039-001 : Multiples vulnérabilités dans OpenOfficeorg (ajout des bulletins des distributions Debian et RedHat.)

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 règlementaire, 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 inexpliqués 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_rubrique62.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.

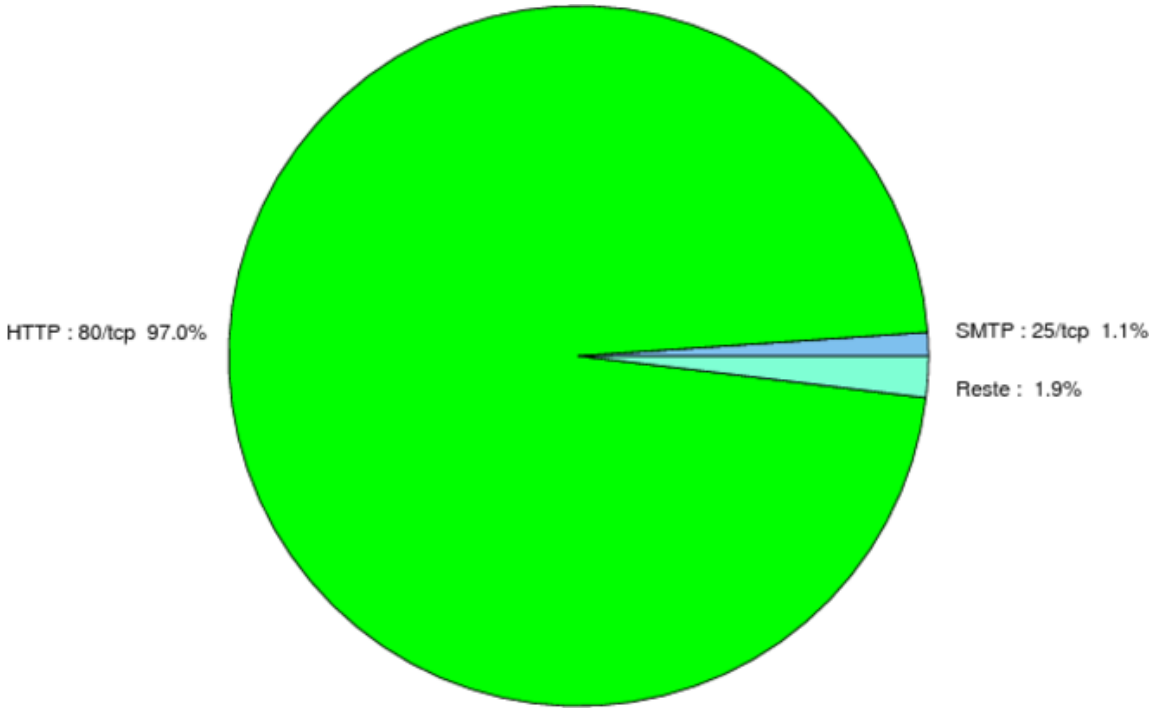

FIG. 1: Répartition relative des ports pour la semaine du 28 janvier au 03 février 2011

port	pourcentage
80/tcp	97.25
25/tcp	1.08
1433/tcp	0.58
135/tcp	0.33
445/tcp	0.32
1080/tcp	0.2
22/tcp	0.19
3389/tcp	0.12
23/tcp	0.03
1434/udp	0.02
4899/tcp	0.01

TAB. 2: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

04 février 2011 version initiale.