



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 18 mars 2011
N° CERTA-2011-ACT-011

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2011-11

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-2011-ACT-011>

Gestion du document

Référence	CERTA-2011-ACT-011
Titre	Bulletin d'actualité 2011-11
Date de la première version	18 mars 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-011.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-011/>

1 Incident de la semaine

Gestion des messages piégés et sensibilisation des utilisateurs

Cette semaine, le CERTA a pu constater que certains utilisateurs ont parfois tendance à transmettre à leurs collègues un courriel dont ils n'arrivent à ouvrir la pièce jointe. Dans le cas présent, cette pièce jointe était piégée par un code malveillant et c'est justement l'arrêt inopiné de l'application qui permet l'exécution du code. Le transfert de courriel et la pièce jointe à des collègues afin que ces derniers testent l'ouverture de la pièce jointe permet ainsi à l'attaquant que son code malveillant soit propagé à un plus grand nombre de victimes.

Le CERTA profite de cette anecdote pour rappeler certains signaux faibles dont la prise en compte peut limiter ou éviter la compromission d'une machine via un document piégé :

- arrêt inopiné de l'application ;
- apparition de fenêtre (notamment d'invite de commandes) ;
- fermeture puis réouverture de l'application en charge de la lecture du document...

Les utilisateurs doivent être sensibilisés à l'ensemble de ces phénomènes pour qu'ils aient le réflexe de remonter ces alertes à leurs responsables informatiques. Il est également important de rappeler aux utilisateurs qu'il faut éviter de tenter de reproduire le problème sur d'autres postes, au risque d'infecter d'autres machines. De même, il est important que les utilisateurs soient sensibilisés au fait de ne pas ouvrir systématiquement toutes les pièces jointes surtout lorsque que l'expéditeur est inconnu ou qu'aucun message n'en est attendu.

Une bonne gestion des mises à jour des applicatifs de bureautique permet également de limiter la surface de vulnérabilité du système d'information.

2 0-day Adobe Flash Player (CVE-2011-0609)

Cette semaine le CERTA a émis une alerte concernant une vulnérabilité non corrigée dans Adobe Flash Player <http://www.certa.ssi.gouv.fr/site/CERTA-2011-ALE-002/index.html>. Cette vulnérabilité non corrigée permet l'exécution de code arbitraire à distance sur les versions récentes d'Adobe Flash Player (9.x et 10.x).

Des attaques utilisant cette vulnérabilité sont activement menées sur l'Internet. Le vecteur d'infection diffère de ce qui est habituellement constaté pour les vulnérabilités Flash. Ici, on ne cherche pas à amener l'utilisateur sur une page Web diffusant un fichier Flash malveillant, mais un courriel est envoyé avec un fichier joint au format Microsoft Excel embarquant le fichier Flash malveillant. Il est en effet tout à fait possible d'embarquer des fichiers au format Flash en utilisant les menus d'Excel. Il est important de préciser que le fichier Excel est le vecteur actuellement observé de cette attaque, mais il est possible que cette vulnérabilité utilise d'autres vecteurs : autres formats MS-Office, PDF, page Web, ou encore fichier SWF brut.

La technologie Flash utilise le langage ActionScript et la machine virtuelle AVM (ActionScript Virtual Machine) servant à l'exécuter. La vulnérabilité se situe dans le vérifieur de *bytecode* ActionScript, dans l'AVM.

Un moyen de contournement pour les utilisateurs de Windows est l'installation du Enhanced Mitigation Evaluation Toolkit (EMET) de Microsoft. Cet outil permet d'activer un certain nombre de protections pour les applications exécutables sélectionnées. Dans le cadre de cette vulnérabilité, il est intéressant de l'activer pour les applications Microsoft Office (en priorité Excel) et pour le navigateur Web. Ces protections comprennent Data Execution Prevention (DEP), Export Address Table Access Filtering (EAF), et HeapSpray pre-allocation. Ces mesures de protection se sont montrées efficaces contre les attaques connues utilisant cette vulnérabilité, notamment parce que ces dernières utilisent la méthode HeapSpray pour se stabiliser.

Adobe a annoncé un correctif pour la semaine du 21 mars 2011. Google Chrome est, quant à lui, déjà corrigé : <http://www.google.com/support/chrome/bin/answer.py?hl=en?answer=95414>. En attendant la sortie du correctif, le CERTA recommande bien sûr de ne pas ouvrir de fichiers suspects, en particulier les fichiers Microsoft Excel que vous pourriez recevoir en pièce jointe d'un courriel.

3 Notes d'information du CERTA

Le CERTA a mis à jour deux notes d'information cette semaine.

3.1 Les systèmes et logiciels obsolètes

Le CERTA recommande continuellement de mettre à jour ses logiciels, d'appliquer les correctifs de sécurité. C'est une mesure élémentaire pour réduire la surface d'attaque offerte aux agresseurs. La conséquence directe est d'abandonner l'utilisation des logiciels (systèmes, applications et extensions diverses) qui ne sont plus maintenus.

Dans le but d'aider sa communauté, le CERTA met régulièrement à jour une note d'information qui indique des systèmes devenus obsolètes.

3.2 Tunnel et pare-feux : une cohabitation difficile

Ce sujet est toujours d'actualité. Les codes malveillants savent utiliser les protocoles admis dans la plupart des PSSI, comme HTTP et HTTPS pour traverser les pare-feux. La mise à jour porte sur l'ajout d'une référence à une circulaire de 2005 contenant des recommandations.

Par ailleurs, le memento de la référence numéro 9 sera bientôt remplacé par un guide de sécurisation accessible en ligne. La note sera mise à jour en conséquence.

3.3 Documentation

- Note d'information du CERTA « Les systèmes et logiciels obsolètes » :
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-003/index.html>
- Note d'information du CERTA « Tunnels et pare-feux : une cohabitation difficile » :
<http://www.certa.ssi.gouv.fr/site/CERTA-2001-INF-003/index.html>

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 11 au 17 mars 2011, le CERTA a émis les avis suivants :

- CERTA-2011-AVI-149 : Vulnérabilité dans Majordomo 2
- CERTA-2011-AVI-150 : Multiples vulnérabilités dans Apple Safari
- CERTA-2011-AVI-151 : Multiples vulnérabilités dans Apple iOS
- CERTA-2011-AVI-152 : Vulnérabilité dans Google Chrome
- CERTA-2011-AVI-153 : Vulnérabilités dans SAP Crystal Reports
- CERTA-2011-AVI-154 : Vulnérabilité dans Check Point SNX, EPS et EPC
- CERTA-2011-AVI-155 : Vulnérabilité dans MIT Kerberos
- CERTA-2011-AVI-156 : Vulnérabilités dans Asterisk

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

- CERTA-2011-AVI-011-001 : Vulnérabilité dans Struts (ajout des références concernant VMware vCO)
- CERTA-2011-AVI-077-001 : Multiples vulnérabilités dans Adobe Flash Player (ajout du bulletin de sécurité de Sun)
- CERTA-2011-AVI-079-005 : Vulnérabilité dans plusieurs implémentations de Java (ajout de la référence au bulletin HP OpenView Network Node Manager)

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_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.

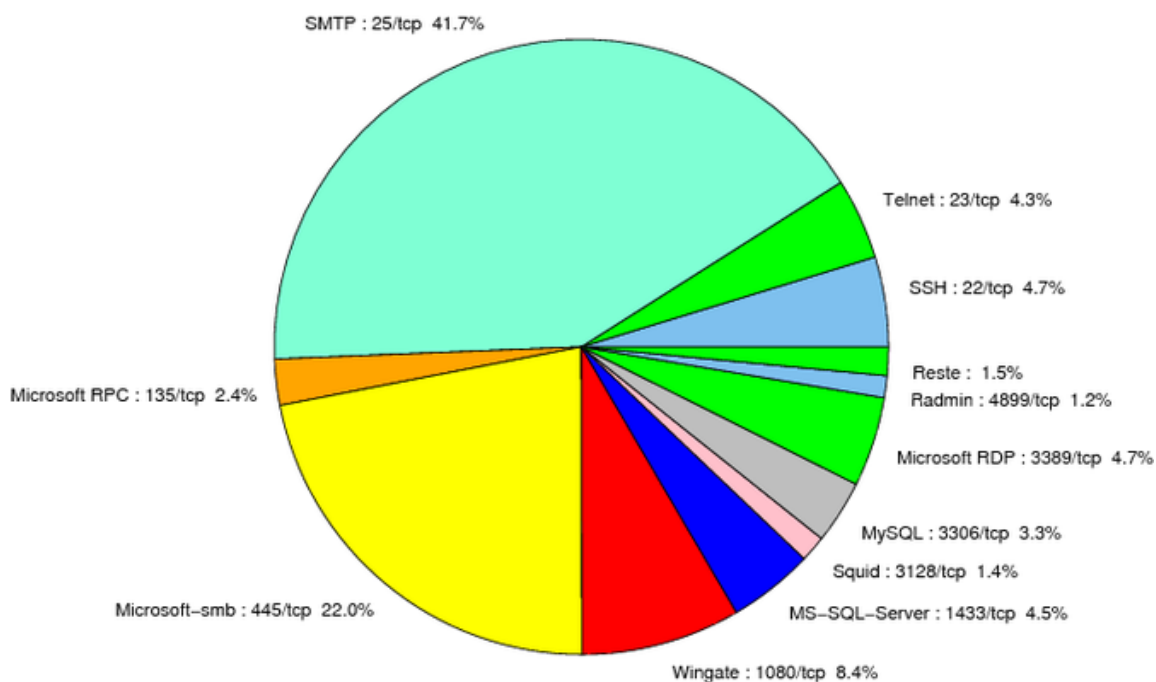


FIG. 1: Répartition relative des ports pour la semaine du 11 au 17 mars 2011

port	pourcentage
25/tcp	41.65
445/tcp	21.97
1080/tcp	8.4
3389/tcp	4.71
1433/tcp	4.48
23/tcp	4.25
3306/tcp	3.33
135/tcp	2.41
3128/tcp	1.38
4899/tcp	1.15
21/tcp	0.92
2967/tcp	0.57
1434/udp	0.11

TAB. 2: Paquets rejetés

Liste des tableaux

1	Gestion du document	1
2	Paquets rejetés	6

Gestion détaillée du document

18 mars 2011 version initiale.