

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2011-50

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-050>

Gestion du document

Référence	CERTA-2011-ACT-050
Titre	Bulletin d'actualité 2011-50
Date de la première version	16 décembre 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-050.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-050/>

1 Incidents de la semaine

1.1 Utilisation imprudente d'un service gratuit externe

Il est tentant d'utiliser des services gratuits en ligne « ponctuellement », sans forcément prendre conscience de toutes les conséquences de cette utilisation.

Dans un cas survenu récemment, un agent de l'administration s'est servi du site pastebin.com, transférant sur celui-ci des données apparemment non-sensibles. Cette utilisation naïve, sans intention de nuire, mais sans avoir la moindre conscience des risques et des impacts, a rendu des contenus accessibles de tout l'Internet, indexables par des moteurs de recherche et non effaçables.

De plus, si les fragments d'informations paraissent peu sensibles, ils permettent d'en apprendre toujours un peu plus sur un organisme et sur ses membres, et de faciliter une approche par ingénierie sociale.

Quelle que soit la raison qui a poussé l'utilisateur à procéder de la sorte, il doit y avoir au préalable une prise de conscience des risques liés à la diffusion d'informations sur des serveurs externes. Le guide de l'ANSSI sur l'externalisation (voir Documentation) est conçu dans l'optique d'une passation de marché pour une prestation, mais les principes qui le sous-tendent sont valables y compris pour une utilisation ponctuelle d'un service externe, fût-il gratuit.

Dans la même optique, celle des services sur l'Internet gratuits, on peut signaler les antivirus gratuits en ligne auxquels il est possible de soumettre un fichier à analyser. L'utilisation de ces services soulèvent plusieurs questions :

- qu'advient-il du document analysé après affichage du verdict (infection détectée ou non) par le serveur ?
- quelles informations connexes (adresse IP, date et heure de soumission, etc.) sont collectées, publiées ou accessibles en mode restreint, et par qui ?

D'autres questions sont intéressantes, concernant la protection de données sensibles (classifiées, personnelles) ou pour la lutte contre l'intelligence économique :

- quelle société opère le service ? La réponse est aisée pour un antivirus proposé par l'éditeur lui-même, mais beaucoup plus difficile dans d'autres cas (ex. : [virscan.org](http://www.virscan.org)) ;
- dans quel(s) pays les données sont-elles transférées ?

La soumission de certains fichiers dépendra des risques que l'organisme assume, et sera de préférence formalisée dans sa PSSI.

Documentation

- *Maîtriser les risques de l'infogérance - Externalisation des systèmes d'information*
http://www.ssi.gouv.fr/IMG/pdf/2010-12-03_Guide_externalisation.pdf

2 Mise à jour mensuelle Microsoft

Cette semaine, Microsoft a publié son ensemble mensuel de correctifs de sécurité. Ce sont ainsi treize bulletins de sécurité qui ont été mis en ligne. Le CERTA rappelle l'impérative nécessité de déployer au plus vite ces mises à jour. Une synthèse des bulletins publiés est disponible dans la section Documentation ci-après.

Il est à noter que le bulletin MS11-087 corrige la vulnérabilité exploitée par le logiciel malveillant Duqu (cf alerte CERTA CERTA-2011-ALE-006).

Documentation

- Synthèse des bulletins de sécurité Microsoft du mois de décembre 2011 :
<http://technet.microsoft.com/fr-fr/security/bulletin/ms11-dec>

3 Rappel des avis émis

Dans la période du 04 décembre au 15 décembre 2011, le CERTA a émis les publications suivantes :

- CERTA-2011-AVI-678 : Vulnérabilité dans Novell ZENworks
- CERTA-2011-AVI-679 : Vulnérabilité dans CA SiteMinder
- CERTA-2011-AVI-680 : Vulnérabilité dans Trend Micro Control Manager
- CERTA-2011-AVI-681 : Vulnérabilité dans Apache Struts
- CERTA-2011-AVI-682 : Vulnérabilités dans Asterisk
- CERTA-2011-AVI-683 : Vulnérabilité dans acpid
- CERTA-2011-AVI-684 : Vulnérabilité dans la gestion des polices TrueType sur Windows
- CERTA-2011-AVI-685 : Vulnérabilité dans Microsoft Office
- CERTA-2011-AVI-686 : Vulnérabilité dans Microsoft Office
- CERTA-2011-AVI-687 : Vulnérabilité dans Microsoft Time
- CERTA-2011-AVI-688 : Vulnérabilités dans Microsoft Publisher
- CERTA-2011-AVI-689 : Vulnérabilité dans Windows Media Player
- CERTA-2011-AVI-690 : Vulnérabilité dans OLE
- CERTA-2011-AVI-691 : Vulnérabilités dans Microsoft PowerPoint
- CERTA-2011-AVI-692 : Vulnérabilité dans Active Directory
- CERTA-2011-AVI-693 : Vulnérabilité dans Microsoft Excel
- CERTA-2011-AVI-694 : Vulnérabilité dans Microsoft Windows
- CERTA-2011-AVI-695 : Vulnérabilité dans le noyau Windows

- CERTA-2011-AVI-696 : Multiples vulnérabilités dans Internet Explorer
- CERTA-2011-AVI-697 : Vulnérabilités dans Adobe ColdFusion
- CERTA-2011-AVI-698 : Vulnérabilités dans Google Chrome
- CERTA-2011-AVI-699 : Multiples vulnérabilités dans Cacti

Durant la même période, les publications suivantes ont été mises à jour :

- CERTA-2011-ALE-006-003 : Exploitation d'une vulnérabilité dans la gestion des polices TrueType sur Windows (ajout du correctif Microsoft)
- CERTA-2011-AVI-531-001 : Multiple vulnérabilités dans Adobe Flash Player (ajout du bulletin Oracle)

4 Actions suggérées

4.1 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.

4.2 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.

4.3 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.

4.4 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.

4.5 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.

4.6 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.

4.7 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

Gestion détaillée du document

16 décembre 2011 version initiale.