

Affaire suivie par :  
CERTA

## BULLETIN D'ACTUALITÉ

### Objet : Bulletin d'actualité 2011-49

---

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-049>

---

### Gestion du document

Référence	CERTA-2011-ACT-049
Titre	Bulletin d'actualité 2011-49
Date de la première version	09 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-049.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-049/>

## 1 Des nouvelles pratiques de fournisseurs de téléchargements

Cette semaine, un message sur la liste de diffusion de développement du logiciel *Nmap* a annoncé que le site Web de Download.com proposait au téléchargement certaines versions des logiciels qui leur sont proposés encapsulées dans un installateur produit par ce site de téléchargement.

Sous prétexte d'assurer un téléchargement « sécurisé » ou encore « plus performant », le visiteur se verra proposer l'installation de barres d'outils, ou encore le changement automatique de la page d'accueil de son navigateur Web. Ces options sont bien entendu activées par défaut, et il faudra que le visiteur soit vigilant lors de l'installation pour demander explicitement de ne pas modifier son système.

Ces pratiques récentes apportent évidemment des bénéfices financiers au site qui installe une barre d'outils, par l'affichage de publicités, ou la redirection de certaines recherches vers des résultats bien définis. Le Bulletin d'Actualité CERTA-2011-ACT-021 rappelle les risques engendrés par ces barres d'outils.

Depuis que cette pratique a été publiquement dénoncée par certains éditeurs de logiciels, il est maintenant proposé aux développeurs de désactiver l'encapsulation dans l'installateur de Download.com. Download.com a également indiqué que tous les logiciels à source ouverte proposés ne sont plus sujets à cette pratique.

Le CERTA recommande, lors du téléchargement d'un logiciel, soit de passer par un fournisseur qui sera soit géré par le système d'exploitation utilisé, soit de se connecter directement au site de l'éditeur. Cette dernière

méthode est d'ailleurs généralement la seule permettant de vérifier la signature cryptographique de l'exécutable récupéré, lorsque celle-ci est disponible.

## Documentation

- Message de la liste de diffusion Nmap dénonçant la pratique :  
<http://seclists.org/nmap-hackers/2011/5>
- Message de Download.com à propos de leur installateur :  
[http://download.cnet.com/8301-2007\\_4-57338809-12/a-note-from-sean-regarding-the-download.com-installer/](http://download.cnet.com/8301-2007_4-57338809-12/a-note-from-sean-regarding-the-download.com-installer/)
- Bulletin d'Actualité du CERTA CERTA-2011-ACT-021 :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2011-ACT-021/>

## 2 Imprimantes en réseau, un tendon d'Achille

Les annonces récentes de fabricants d'imprimantes nous rappellent que ces appareils ne sont plus des périphériques « passifs » mais des systèmes à part entière. Leurs vulnérabilités peuvent avoir un impact sur tous les systèmes d'information sur lesquels elles sont connectées.

### 2.1 Risques signalés récemment

Les imprimantes en réseau sont des ordinateurs à part entière, avec des fonctions de serveur, pour envoyer les documents à imprimer, mais également pour configurer ces imprimantes, les mettre à jour à distance et en consulter divers éléments.

Les fabricants Xerox et HP viennent de rappeler que des mots de passe doivent être positionnés et différents des mots de passe usine pour protéger le mécanisme de mise à jour du micrologiciel (*firmware*). La même recommandation s'étend à tous les matériels (imprimantes, copieurs multifonctions, etc.) de toutes les marques dès lors que des fonctions de consultation (ex. : fichiers soumis) ou de modification existent.

La protection par mot de passe est un minimum. Elle est insuffisante quand le mot de passe transite en clair sur le réseau local. La mise en place d'un tunnel chiffrant, au moins jusqu'à un équipement proche de l'imprimante est alors complémentaire. Ce tunnel protégera également les documents transmis pour impression.

D'autres moyens sont complémentaires, comme l'accès à l'imprimante restreint à certains ordinateurs.

### 2.2 Impacts sur le SI

L'impact des vulnérabilités sur les imprimantes peut être évident ou, au contraire, très indirect :

- un déni de service par modification de la configuration ;
- la fuite d'information, par capture d'un flux non chiffré vers l'imprimante, par accès non autorisé au stockage sur l'imprimante ou par utilisation abusive d'une fonction de réimpression ;
- un comportement dangereux (surchauffe, incendie) ou non (gaspillage de consommables) par la modification du micrologiciel ;
- infection des postes de travail, par dépôt d'une réserve discrète de programmes malveillants, sur ce périphérique que l'on ne pensera pas à désinfecter lors du traitement d'une intrusion d'ampleur. Ce dépôt peut se faire, par exemple, par l'exploitation d'une vulnérabilité présente sur l'un des serveurs.

## Documentation

- Bulletin de sécurité HP c03102449 du 30 novembre 2011 :  
<http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c03102449>
- Rappel de sécurité de Xerox du 30 novembre 2011 :  
<http://www.xerox.com/information-security/enus.html>
- Référence CVE CVE-2011-4161 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-4161>

### 3 Alerte du CERTA concernant une vulnérabilité dans Adobe Reader

Le 6 décembre 2011, l'éditeur Adobe a publié une alerte portant sur une vulnérabilité dans les produits Adobe Reader et Acrobat. Selon l'éditeur, il semble que cette vulnérabilité soit actuellement exploitée sur l'Internet au moyen d'un fichier PDF spécialement conçu.

Afin d'offrir un rendu en trois dimensions dans des documents PDF, certains produits Adobe interprètent le format U3D. La vulnérabilité précitée est causée par une erreur dans le traitement des fichiers au format U3D.

L'exploitation de cette vulnérabilité permet à une personne malveillante d'exécuter du code arbitraire à distance au moyen d'un fichier au format PDF spécialement construit.

Le CERTA recommande d'appliquer les contournements provisoires décrits dans son alerte CERTA-2011-ALE-008 du 07 décembre 2011 afin de limiter l'impact lié à l'exploitation de cette vulnérabilité.

### Documentation

- Alerte CERTA-2011-ALE-008 du 07 décembre 2011 :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2011-ALE-008/>
- Alerte de sécurité Adobe APSA11-04 du 6 décembre 2011 :  
<http://www.adobe.com/support/security/advisories/apsa11-04.html>
- Référence CVE CVE-2011-2462 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2462>

### 4 Rappel des avis émis

Dans la période du 03 décembre au 08 décembre 2011, le CERTA a émis les publications suivantes :

- CERTA-2011-ALE-007 : Vulnérabilité dans ftpd et ProFTPD sur FreeBSD
- CERTA-2011-ALE-008 : Vulnérabilité dans Adobe Reader et Acrobat
- CERTA-2011-AVI-670 : Vulnérabilité dans Adobe Flex
- CERTA-2011-AVI-671 : Vulnérabilités dans JBoss
- CERTA-2011-AVI-672 : Vulnérabilité dans Blue Coat ProxyAV
- CERTA-2011-AVI-673 : Vulnérabilité dans libXfont
- CERTA-2011-AVI-674 : Vulnérabilité dans MIT Kerberos
- CERTA-2011-AVI-675 : Vulnérabilités dans Opera
- CERTA-2011-AVI-676 : Vulnérabilité dans Foxit Reader
- CERTA-2011-AVI-677 : Vulnérabilité dans ISC DHCP

### 5 Actions suggérées

#### 5.1 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.

## **5.2 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.

## **5.3 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.

## **5.4 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.

## **5.5 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.

## **5.6 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.

## **5.7 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](http://www.ssi.gouv.fr/site_rubrique62.html)

## **Gestion détaillée du document**

09 décembre 2011 version initiale.