



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 25 novembre 2011  
N° CERTA-2011-ACT-047

Affaire suivie par :  
CERTA

## BULLETIN D'ACTUALITÉ

**Objet : Bulletin d'actualité 2011-47**

---

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-047>

---

### Gestion du document

Référence	CERTA-2011-ACT-047
Titre	Bulletin d'actualité 2011-47
Date de la première version	25 novembre 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-047.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-047/>

## 1 Encapsulation et aveuglement des outils de sécurité

La possibilité qu'offrent les logiciels d'encapsuler un objet au format X dans un fichier au format Y devient un handicap pour les produits de sécurité. Cette imbrication de formats peut être une fonction primaire (création d'archives) ou une fonctionnalité destinée à élargir les capacités premières d'un logiciel (importation d'image de tout format dans un traitement de texte).

Quelques exemples vont montrer comment cette capacité est favorable aux agresseurs informatiques et nuisible aux défenseurs.

### 1.1 Exemples

Le premier exemple est la création itérative d'archives. Le virus test EICAR est reconnu par tous les produits antivirus, quand il est dans un fichier plat. Mis dans une archive au format ZIP, il est encore détecté. Cette archive peut être à son tour zippée ou mise dans une archive RAR, ZOO ou autre. En itérant cette encapsulation, le taux de détection par les antivirus dans leur configuration d'usine diminue pour finir par s'annuler. La raison peut être un défaut de reconnaissance de la charge malveillante ou simplement un arrêt du désarchivage par l'antivirus.

Le deuxième exemple est une série de problèmes d'analyseurs de formats. Le CERTA a émis de nombreux avis et même une alerte sur les antivirus pour le même motif. La malformation d'un fichier, souvent une archive, ZIP, ZOO, RAR..., n'est pas correctement gérée par l'analyseur utilisé par l'antivirus. Dans cette série de vulnérabilités, l'échec de l'analyse se traduit par l'acceptation du fichier archive sans même analyser les fichiers qu'il contient.

Le troisième exemple se rapporte aux formats de fichiers rarement utilisés mais manipulés par des logiciels très courants. À l'installation de ces logiciels, ces formats sont automatiquement associés. Le double-clic sur le fichier dans le navigateur provoque automatiquement l'ouverture de ce fichier au format rarement utilisé. Pour des raisons de performance ou à cause du coût de développement des analyseurs de formats, ces fichiers ne sont pas analysés par certains outils de sécurité. Il est alors aisé pour les cyberattaquants de les utiliser pour traverser des défenses périmétriques et atteindre les postes de travail équipés du logiciel qui traitera ces formats.

Le dernier exemple est l'utilisation d'une archive chiffrée pour empêcher l'analyse du contenu.

## 1.2 Recommandations

Face à cela, quelques précautions sont utiles, dans la mesure où la politique de sécurité le permet.

Tout d'abord, et le CERTA le martelle sans cesse, les logiciels doivent être mis à jour. Cela augmente l'efficacité des protections périphériques et diminue la surface d'attaque sur les postes de travail et les serveurs.

Ensuite, il convient d'adapter les lignes défenses à la surface d'attaque des cibles potentielles.

Ainsi, si un format de fichier X n'est pas traité sur les postes de travail, car inutile aux métiers, alors il doit être bloqué par les défenses. Le rejet des fichiers de ce type peut se faire sur les passerelles et les sas. Le rejet doit également s'appliquer en cas d'encapsulation dans des archives ou dans des conteneurs. De plus, si ce format n'est pas utile, alors l'ouverture automatique par un logiciel de lecture de ce format doit être remplacée par une ouverture par un logiciel de base (un éditeur de texte brut, par exemple), non pas pour un rendu plus ou moins fidèle, mais simplement pour empêcher l'exploitation d'une possible vulnérabilité du lecteur de ce format.

Toujours dans la recherche de cohérence, la politique de sécurité doit déterminer l'attitude à adopter face à un fichier ou à un objet dont l'analyse est impossible. La décision est-elle libérale (le fichier est alors accepté) ou restrictive (ce qui n'est pas analysé est jugé hostile et bloqué) ? Certains organismes mettent en quarantaine les fichiers chiffrés et ont des procédures particulières pour leur transfert. D'autres services laissent passer ces fichiers, s'en remettant à d'autres niveaux de défense.

Dans le cas d'un antivirus qui annonce se limiter à une certaine profondeur (souvent paramétrable) des archives, la décision prise par celui-ci en cas de profondeur supérieure est rarement explicite. Il est alors souhaitable de disposer d'un système complémentaire qui applique, pour ces profondeurs d'archives, une décision conforme à la PSSI.

## 2 VNC : vulnérabilités et contre-mesures

*Virtual Network Computing* (VNC) est un système qui permet de contrôler un ordinateur à distance tout en affichant son interface graphique. VNC se base sur le protocole *remote frame-buffer* (RFB). Malheureusement, ce protocole utilise un système d'authentification relativement faible et ne propose pas de méthodes pour chiffrer les connexions entre le client et le serveur. Certaines implémentations VNC ajoutent et proposent des mécanismes de chiffrement et d'authentification. Cependant, les implémentations VNC qui se reposent seulement sur le protocole RFB pour ces mécanismes de sécurité sont potentiellement vulnérables à des attaques par recherche exhaustive ou à l'écoute passive de sessions.

Un moyen efficace pour remédier à ce problème est de faire passer la session VNC dans un tunnel sécurisé fourni, par exemple, par IPsec ou SSH. Voici un exemple utilisant SSH :

- sur l'ordinateur accueillant le serveur VNC :
  1. configurer le serveur VNC de manière à ce qu'il écoute seulement sur l'interface de bouclage (*loop-back*) à l'adresse locale 127.0.0.1 et, par exemple, sur le port 5900,
  2. mettre en place un serveur SSH ;
- sur la machine cliente :
  1. entrer la commande suivante qui permet de rediriger le trafic arrivant sur le port local 5900 de la machine cliente, vers le port 5900 du serveur qui héberge le serveur VNC, en passant par la session

SSH : ssh -L5900:127.0.0.1:5900 vncuser@vncserver. La session VNC entre la machine cliente et la machine serveur passera ainsi par la session SSH ;

2. dans l'application cliente VNC, définir le serveur comme étant à l'adresse 127.0.0.1 sur le port 5900.

### 3 Rappel des avis émis

Dans la période du 18 au 24 novembre 2011, le CERTA a émis les publications suivantes :

- CERTA-2011-AVI-646 : Vulnérabilité dans iTunes
- CERTA-2011-AVI-647 : VMware vCenter Update Manager
- CERTA-2011-AVI-648 : Vulnérabilité dans nginx
- CERTA-2011-AVI-649 : Multiples vulnérabilités dans SAP NetWeaver
- CERTA-2011-AVI-650 : Vulnérabilité dans Juniper Junos
- CERTA-2011-AVI-651 : Vulnérabilités dans HP Network Node Manager
- CERTA-2011-AVI-652 : Vulnérabilités dans SAP
- CERTA-2011-AVI-653 : Vulnérabilité dans Ruby on Rails
- CERTA-2011-AVI-654 : Vulnérabilités dans SPIP
- CERTA-2011-AVI-655 : Vulnérabilité dans Dovecot
- CERTA-2011-AVI-656 : Multiples vulnérabilités dans RealPlayer
- CERTA-2011-AVI-657 : Vulnérabilités dans TikiWiki
- CERTA-2011-AVI-658 : Vulnérabilité dans Ubuntu Software Center
- CERTA-2011-AVI-659 : Vulnérabilité dans IBM Lotus Mobile Connect
- CERTA-2011-AVI-660 : Vulnérabilité dans CA Directory
- CERTA-2011-AVI-661 : Vulnérabilité dans syslog-ng Premium Edition
- CERTA-2011-AVI-662 : Vulnérabilités dans TYPO3
- CERTA-2011-AVI-663 : Vulnérabilités dans Tomcat pour HP-UX
- CERTA-2011-AVI-664 : Multiples vulnérabilités dans FFmpeg
- CERTA-2011-AVI-665 : Vulnérabilité dans System Administration Manager pour systèmes HP-UX
- CERTA-2011-AVI-666 : Vulnérabilité dans le module Digest pour Perl

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

- CERTA-2011-AVI-490-002 : Vulnérabilité dans Apache httpd (ajout de la référence au 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](http://www.ssi.gouv.fr/site_rubrique62.html)

## **Gestion détaillée du document**

25 novembre 2011 version initiale.