Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 28 octobre 2011
N° CERTA-2011-ACT-043

**Affaire suivie par :**
CERTA

# BULLETIN D'ACTUALITÉ

## Objet : Bulletin d'actualité 2011-43



## Gestion du document

| | |
|---|---|
| Référence | CERTA-2011-ACT-043 |
| Titre | Bulletin d'actualité 2011-43 |
| Date de la première version | 28 octobre 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-043.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-043/

## 1 Exploitation malveillante d'une fonctionnalité du protocole SSL afin de provoquer un déni de service

Cette semaine le CERTA a publié l'alerte CERTA-2011-ALE-005 concernant l'exploitation malveillante de fonctionnalités du protocole SSL/TLS. Notre alerte réagit à la publication d'articles et d'outils permettant à un attaquant de provoquer un déni de service de services applicatifs critiques mettant en œuvre le protocole SSL/TLS.

À ce jour, le CERTA n'a pas constaté d'attaques utilisant spécifiquement cette technique ou ces outils.

### Documentation

– Alerte CERTA CERTA-2011-ALE-005 :
http://www.certa.ssi.gouv.fr/site/CERTA-2011-ALE-005/

## 2 Code malveillant Duqu : erratum

Dans le numéro précédent du bulletin d'actualité du CERTA, une coquille s'est glissée. La version du bulletin sur le site du CERTA a été corrigée. L'adresse IP vers laquelle des ordinateurs infectés par Duqu tentaient de se connecter est bien **206.183.111.97**.

Attention toutefois.

La découverte de variantes du programme malveillant ne doit pas focaliser tous les regards vers cette seule adresse IP. D'autres adresses ou des noms de sites pourraient être utilisées par ces variantes.

Il convient de surveiller les trafics entrants et sortants et d'étudier les comportements anormaux (source, destination, protocole, volume, horaire, séquence, URL...).

### Documentation

- Document du CERTA CERTA-2011-ACT-042 du 21 octobre 2011 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2011-ACT-042/index.html

## 3 Microsoft Office 2007 SP3 et cycle de vie des Service Packs

Microsoft a publié cette semaine le Service Pack 3 pour Office 2007.

Comme tout Service Pack celui-ci inclus, entre autres, toutes les mises à jours de sécurité cumulatives (jusqu'en septembre 2011).

Pour rappel, lors de la sortie d'un Service Pack, le Service Pack précédent reste supporté 12 mois (pour Office). Office 2007 SP2 ne sera donc plus supporté (y compris pour les mises à jour de sécurité) à partir de novembre 2012.

### Documentation

- Article technique Microsoft pour Office Service Pack 3 :
  http://support.microsoft.com/kb/2526086/fr
- Politique de support Microsoft:
  http://support.microsoft.com/gp/lifeselect

## 4 Rappel des avis émis

Dans la période du 21 au 27 octobre 2011, le CERTA a émis les publications suivantes :

- CERTA-2011-ALE-005 : Exploitation malveillante d'une fonctionalité du protocole SSL
- CERTA-2011-AVI-581 : Vulnérabilité dans IBM Websphere
- CERTA-2011-AVI-582 : Vulnérabilités dans plusieurs produits Symantec
- CERTA-2011-AVI-583 : Vulnérabilité dans CiscoWorks Common Services
- CERTA-2011-AVI-584 : Vulnérabilités dans Cisco Show and Share
- CERTA-2011-AVI-585 : Vulnérabilités dans HP MFP Digital Sending Software
- CERTA-2011-AVI-586 : Multiples vulnérabilités dans les produits Oracle
- CERTA-2011-AVI-587 : Vulnérabilités dans Splunk
- CERTA-2011-AVI-588 : Vulnérabilités dans HP Data Protector Notebook Extension
- CERTA-2011-AVI-589 : Vulnérabilités dans LibreOffice
- CERTA-2011-AVI-590 : Vulnérabilité dans OCS Inventory
- CERTA-2011-AVI-591 : Multiples vulnérabilités dans FFmpeg
- CERTA-2011-AVI-592 : Vulnérabilités dans Linux-PAM
- CERTA-2011-AVI-593 : Vulnérabilités dans Google Chrome
- CERTA-2011-AVI-594 : Vulnérabilités dans Alcatel OmniTouch Instant Communication Suite
- CERTA-2011-AVI-595 : Vulnérabilités dans MIT Kerberos
- CERTA-2011-AVI-596 : Vulnérabilité dans McAfee Web Gateway

# 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 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.

## 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 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.

### 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

## Gestion détaillée du document

**28 octobre 2011** version initiale.