Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 23 décembre 2011
N° CERTA-2011-ACT-051

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2011-51

Gestion du document

Référence	CERTA-2011-ACT-051
Titre	Bulletin d'actualité 2011-51
Date de la première version	23 décembre 2011
Date de la dernière version	–
Source	–
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-051.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-051/

1 Pour passer de bonnes fêtes de fin d'année

Le CERTA souhaite à ses lecteurs d'excellentes fêtes de fin d'année.

Pour éviter de les gâcher ou d'engâcher les lendemains, le CERTA rappelle quelques conseils de prudence :
- être vigilant lors de la récéption de cartes de voeux sous forme électronique, en particulier (mais pas seulement) au format Flash. Même un site de bonne réputation peut être compromis et vous transmettre, à son insu et à celui de vos correspondants, des codes malveillants ;
- être vigilant à la récéption des courriels de manière générale. L'adresse d'expéditeur peut être fausse et le courriel ne pas provenir de son expéditeur affiché. Les spammeur et les attaquant cherchant à construire des *botnets* utilisent l'actualité, en particulier les fêtes de fin d'années ;
- être vigilant avant de connecter un cadeau électronique (clef USB publicitaire, baladeur MP3, cadre photo numérique, disque externe...). Le CERTA a régulièrement connaissance d'appareils neufs contenant des programmes malveillants et l'a relaté dans ses bulletins d'actualité ;
- bien sur, dans le respect de la PSSI, ne pas connecter ces objets privés sur le SI de son entreprise ou de son adminsitration.

Sans prises de précautions, les lendemains de fêtes peuvent être difficiles, pas seulement pour le tube digestif.

1.1 Documentation

- Mesures de prévention relatives à la messagerie :
  http://www.certa.ssi.gouv.fr/site/CERTA-2000-INF-002
- Mise en garde au sujet des messages de voeux :
  http://www.certa.ssi.gouv.fr/site/CERTA-2000-REC-002
- Risques associés aux clés USB :
  http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-006

2 Incidents de la semaine

Le CERTA a été alerté cette semaine de plusieurs vagues d'attaques par des courriels piégés particulièrement soignés qui ciblent des grandes entreprises francaises et étrangères. Les messages étaient adaptés à chaque cible : l'adresse de l'expéditeur (usurpée) était en général une adresse interne à l'entreprise, le contenu du message pertinent, et les courriels avaient tous une pièce jointe crédible au format PDF. Dans au moins un cas, le fichier PDF était un document disponible sur le site internet de l'entreprise. Dans tous les cas, le contenu malveillant était dans la pièce jointe. La vulnérabilité citée dans l'alerte CERTA-2011-ALE-008-001 a été utilisée. L'ouverture du fichier par l'utilisateur déclenche l'exploitation qui va réaliser une série d'actions sur la machine de l'utilisateur, dont l'installation d'un Cheval de Troie qui va ensuite chercher des ordres sur l'Internet, donnant le contrôle de la machine à l'attaquant.

Lors des premières vagues d'attaques autour du 13 décembre, la vulnérabilité mentionnée ci-dessus n'était pas encore corrigée par l'éditeur et la plupart des anti-virus ne détectaient pas le contenu malveillant. Depuis, Adobe a publié un correctif pour les versions 9.x qu'il est donc extrèmement conseillé de déployer au plus vite. Le correctif pour les versions 10.x n'est toujours pas disponible mais une solution de contournement existe (activation des modes de protection, se référer au bulletin d'alerte du CERTA).

Ces attaques n'ont pu être détectées que par la vigilance des utilisateurs qui ont trouvé le message suspect et l'ont remonté via leur chaîne SSI.

Face à ces attaques, le CERTA recommande :

- l'installation des correctifs ou la mise en place des solutions de contournement si ce n'est pas déjà fait ;
- la mise en place de mesures organisationnelles et techniques de filtrage des courriels dont l'expéditeur est une adresse interne, mais qui arrivent sur la passerelle Internet de l'entreprise ;
- la sensibilisation des utilisateurs ;
- la surveillance des flux sortants.

3 Publication d'une mise à jour de sécurité Microsoft Active Directory

Le 13 décembre, Microsoft a publié la mise à jour MS11-095. Cette mise à jour est évaluée « Importante » selon les critères d'évaluation de Microsoft.

Le CERTA souhaite attirer votre attention sur la sévérité exceptionnelle de cette mise à jour. En effet, une exploitation réussie de cette faille permet la prise de contrôle totale de toutes les machines membres de ce domaine.

De plus, Microsoft évalue le risque de développement d'un programme d'exploitation fonctionnel à « probable ».

Dans un système d'information s'appuyant sur les technologies Microsoft, l'Active Directory constitue la pierre angulaire de la sécurité de l'entreprise et il convient d'investir particulièrement dans sa protection. En conséquence, le CERTA recommande l'application de cette mise à jour aussi rapidement que possible.

De manière plus générale, les mises à jours doivent être régulièrement installées sur les contrôleurs de domaine et la surface d'attaque de ces derniers doit être strictement limitée :

- pas de cohabitation avec des fonctions applicatives ;
- logiciels d'administration réduits au strict minimum ;
- contrôle strict des services Windows actifs.

4 Rappel des avis émis

Dans la période du 16 décembre au 22 décembre 2011, le CERTA a émis les publications suivantes :

- CERTA-2011-AVI-700 : Vulnérabilités dans Splunk

– CERTA-2011-AVI-701 : Vulnérabilité dans RSA SecurID Software Token
– CERTA-2011-AVI-702 : Vulnérabilités dans AIX
– CERTA-2011-AVI-703 : Vulnérabilités dans JBoss
– CERTA-2011-AVI-704 : Vulnérabilité dans un produit Hitachi
– CERTA-2011-AVI-705 : Vulnérabilités dans Adobe Reader et Acrobat Reader
– CERTA-2011-AVI-706 : Vulnérabilité dans OpenPAM
– CERTA-2011-AVI-707 : Vulnérabilité dans EMC RSA Adaptative Authentication On-Premise
– CERTA-2011-AVI-708 : Vulnérabilité dans Intel TXT (solution de sécurité de processeurs Intel) SINIT
– CERTA-2011-AVI-709 : Multiples vulnérabilités dans Nagios XI
– CERTA-2011-AVI-710 : Vulnérabilité dans IBM Tivoli Federated Identity Manager
– CERTA-2011-AVI-711 : Vulnérabilité dans bzexe
– CERTA-2011-AVI-712 : Vulnérabilités dans les produits Mozilla
– CERTA-2011-AVI-713 : Vulnérabilité dans VLC media player
– CERTA-2011-AVI-714 : Vulnérabilité dans PuTTY
– CERTA-2011-AVI-715 : Vulnérabilité dans Tiki Wiki
– CERTA-2011-AVI-716 : Vulnérabilité dans le pilote NVIDIA Stereoscopic 3D

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

– CERTA-2011-ALE-008-001 : Vulnérabilité dans Adobe Reader et Acrobat (publication d'un correctif pour les versions 9)

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

23 décembre 2011 version initiale.