Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 13 janvier 2012
N° CERTA-2012-ACT-002

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2012-02

Gestion du document

Référence	CERTA-2012-ACT-002
Titre	Bulletin d'actualité 2012-02
Date de la première version	13 janvier 2012
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.

1 Attention à l'inclusion de code de source tierce

Un récent incident traité par le CERTA concernait un site diffusant du contenu malveillant. Celui-ci consistait en un code JavaScript redirigeant le navigateur de la victime vers une adresse IP différente de celle du serveur Web, qui ensuite tentait de fournir une charge utile malveillante.

Après investigation, il s'est révélé que ce code n'avait pas été ajouté sur les pages Web suite à une compromission du serveur. Un module JavaScript permettant d'afficher une gallerie interactive avait été téléchargée sur un site proposant des services d'hébergement et de gestion de développement de logiciels.

C'est le code initial, mis à disposition par le créateur du module JavaScript qui avait été détourné de son usage principal. Un attaquant a pu éditer le code du module de gallerie, et insérer son code supplémentaire, obfusqué. Pendant plusieurs semaines, à chaque fois qu'un développeur de site voulait récupérer le module, il installait donc, à son insu, du code malveillant.

Le CERTA rappelle qu'il convient d'être prudent lorsque du code tiers est inclus dans un projet quel qu'il soit, même lorsque la source paraît être de confiance.

2 Mise à jour mensuelle Microsoft

Cette semaine, Microsoft a publié plusieurs correctifs de sécurité. Sur les sept bulletins édités, un est jugé critique par Microsoft et les six autres sont considérés comme importants.

Les vulnérabilités corrigées permettent :

- une exécution de code arbitraire à distance ;
- une élévation de privilège ;
- une atteinte à la confidentialité des données ;
- une injection de code indirecte à distance.

Le CERTA recommande l'application de ces mises à jour dès que possible.

Documentation

- Synthèse des bulletins de sécurité Microsoft du mois de janvier 2012 :
  http://technet.microsoft.com/fr-fr/security/bulletin/ms12-jan

3 FreeBSD, nouvelle branche et fins de support

Le projet FreeBSD vient d'annoncer la sortie de la version 9.0, donc la création d'une nouvelle branche.

Le CERTA en profite pour rappeler que la sortie d'une nouvelle branche s'accompagne rapidement de la fin du support d'une branche plus ancienne, et ce, quel que soit l'éditeur ou le projet.

La fin de support signifie la migration impérative vers des versions maintenues. Cette migration est toujours un projet d'ampleur, afin de s'assurer de l'absence de régressions ou de remédier à celles-ci. Il faut donc anticiper ces fins de support.

Dans le cas de FreeBSD, trois fins de support son annoncées pour 2012 :

- le 31 mars 2012 : FreeBSD 7.3 ;
- le 31 juillet 2012 : FreeBSD 8.1 ;
- le 31 juillet 2012 : FreeBSD 8.2.

Documentation

- Liste des versions supportées par le projet FreeBSD :
  http://www.freebsd.org/security/security.html#sup

4 Rappel des avis émis

- CERTA-2012-AVI-004 : Multiples vulnérabilités dans Google Chrome
- CERTA-2012-AVI-005 : Vulnérabilité dans les imprimantes HP LaserJet P3015
- CERTA-2012-AVI-006 : Multiples vulnérabilités dans OpenSSL
- CERTA-2012-AVI-007 : Vulnérabilité dans le noyau Microsoft Windows
- CERTA-2012-AVI-008 : Vulnérabilité dans le gestionnaire de liaisons de Microsoft Windows
- CERTA-2012-AVI-009 : Vulnérabilité dans le processus CSRSS de Windows
- CERTA-2012-AVI-010 : Vulnérabilités dans Windows Media
- CERTA-2012-AVI-011 : Vulnérabilité dans Microsoft Windows
- CERTA-2012-AVI-012 : Vulnérabilité dans les protocoles SSL/TLS dans Microsoft Windows
- CERTA-2012-AVI-013 : Vulnérabilité dans Microsoft AntiXSS
- CERTA-2012-AVI-014 : Vulnérabilités dans Adobe Reader et Adobe Acrobat

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

- CERTA-2011-ALE-008-002 : Vulnérabilité dans Adobe Reader et Acrobat (publication d'un correctif pour les versions 10)

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

13 janvier 2012 version initiale.