Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 10 juillet 2012
N° CERTA-2012-ACT-027-001

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2012-27

Gestion du document

Référence	CERTA-2012-ACT-027-001
Titre	Bulletin d'actualité 2012-27
Date de la première version	06 juillet 2012
Date de la dernière version	10 juillet 2012
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 Installations accidentelles de Skype

Skype est une application de téléphonie sur IP, capable de contourner les pare-feux et qui chiffre son trafic sans possibilité d'inspection des données envoyées. De plus, la nature par-à-pair du réseau Skype permet à un poste de devenir nœud de transit à son insu. Ces comportements peuvent occasionner des fuites de données sensibles.

Suite à une récente erreur de *Microsoft*, les serveurs de mises à jour *WSUS* ont proposé le déploiement du logiciel de téléphonie *Skype* (acquis par Microsoft en 2012). Le logiciel *Skype* a été déployé sur toutes les machines clientes de *WSUS*, lorsque le déploiement des mises à jour était automatique sans approbation de l'administrateur. Ce problème a concerné les postes sur lesquels *Skype* n'était pas préalablement installé.

Le CERTA attire l'attention des responsables SSI sur le fait qu'un tel logiciel peut être contraire à la PSSI en vigueur dans l'entreprise. La circulaire n1289 publiée sur *Legifrance* le 9 août 2005 recommande de ne pas installer ce logiciel sur les réseaux sensibles. Pour les postes concernés, une manipulation est décrite sur les forums Technet afin de désinstaller *Skype* via l'outil *PsExec*.

Documentation :

– Désinstallation de *Skype* via l'outil *PsExec* :
https://social.technet.microsoft.com/Forums/en-SG/winserverwsus/thread/74a93b2b-e820-40ef-a45d-2815b57d164e

2 Publication d'un rapport sur la résilience de l'Internet

Un rapport intitulé « Résilience de l'Internet - 2011 : état des lieux » a été publié le 22 juin 2012 par l'ANSSI et l'Association française pour le nommage Internet en coopération (AFNIC) suite à une étude menée conjointement. Ce rapport propose un certain nombre d'indicateurs et de mesures de la résilience [1] en se basant sur l'analyse des protocoles BGP et DNS, afin de mieux comprendre la situation actuelle.

Un niveau de résilience optimal de l'Internet est aujourd'hui indispensable pour le bon fonctionnement des institutions et de l'activité économique et sociale. En effet, les nombreux exemples d'entreprises victimes de pannes ou d'attaques parfois massives montrent l'importance de la prise en compte de la résilience lors des déploiements.

Le CERTA recommande la lecture de ce rapport et préconise l'application des bonnes pratiques qui y figurent.

Documentation :

– Rapport « Résilience de l'Internet - 2011 : état des lieux » :
http://www.ssi.gouv.fr/IMG/pdf/rapport-obs-20120620.pdf

3 Décryptement des clés par des ressources PKCS#11

Bon nombre de dispositifs de sécurité actuels, tels que les cartes à puce, les clés USB ou encore les HSM (*Hardware Security Modules*), disposent, parmi leurs fonctionnalités, d'interfaces leur fournissant des fonctions d'import/export de clés cryptographiques chiffrées. Ces mécanismes permettent notamment de conserver les clés sur une zone externe de stockage en cas d'effacement ou de perte des données initiales.

Le standard PKCS#11 est l'un des plus couramment utilisés pour concevoir les interfaces de tels dispositifs. Des chercheurs ont récemment présenté des attaques sur certaines implémentations faibles du standard PKCS#11, qui offrent à l'attaquant l'accès à ce que l'on appelle un « oracle de vérification de *padding* ». Les messages d'erreur renvoyés en cas d'import de données mal formatées peuvent être utilisés par l'attaquant pour reconstituer les valeurs des clés chiffrées. Ces attaques sont réalisables lorsque la clé importée est chiffrée d'une des manières suivantes :

– avec un chiffrement à clé publique RSA avec un *padding* PKCS#1 v1.5 ;
– avec un chiffrement symétrique utilisant le mode CBC-pad.

Il est connu depuis plus de dix ans que des implémentations de ces deux méthodes sont respectivement vulnérables aux attaques de Bleichenbacher et de Vaudenay – pour peu que des messages d'erreur soient envoyés lorsque des anomalies de formatage sont détectées au cours du déchiffrement. Les chercheurs proposent ici des variations de l'attaque originale de Bleichenbacher qui conduisent, dans certains cas, à des améliorations substantielles de son efficacité.

Les chercheurs ont mis en œuvre ces attaques sur un certain nombre de dispositifs de sécurité actuels et sont parvenus à retrouver les clés chiffrées, exportées sous forme chiffrée, en réalisant un nombre limité d'appels à la fonction d'import. Cependant, leur document ne fournit pas suffisamment d'informations pour connaître la portée pratique exacte des attaques constatées et la nature des clés qu'elle permet de compromettre. Cela dépend fortement des attributs des différentes clés et des options retenues dans les implémentations du standard PKCS#11.

On peut ainsi retenir que dès lors qu'un algorithme possède des vulnérabilités, même théoriques et a priori complexes à exploiter, il est souvent préférable de ne plus l'utiliser. En effet, ce type d'attaque révèle des défauts de conception de l'algorithme et peut, bien souvent par la suite, ouvrir la voie à des attaques plus élaborées et/ou plus efficaces à mettre en œuvre.

Documentation :

– Document de recherche « *Efficient Padding Oracle Attacks On Cryptographic Hardware* » :
http://hal.inria.fr/docs/00/70/47/90/PDF/RR-7944.pdf

4 Fin de la saga DNS Changer

Dans un article du bulletin d'actualité CERTA-2012-ACT-010, le CERTA indiquait la prolongation des services fournis par l'*Internet Storm Center* (ISC) jusqu'au 9 juillet 2012. Ces services permettent aux ordinateurs infectés

1. la résilience de l'Internet est définie comme sa capacité à fonctionner et revenir à l'état nominal suite à des incidents

par le code malveillant *DNS Changer* de conserver un accès à des serveurs DNS non malveillants. Pour plus d'information sur ce code malveillant, vous pouvez vous reporter au bulletin d'actualité CERTA-2012-ACT-008.

Les ordinateurs infectés par *DNS Changer* ne pourront donc plus accéder à certains services de l'Internet à partir du 9 juillet. Selon le *DNS Changer Working Group* (DCWG), le nombre d'adresses IP françaises concernées est de plus de 10,000.

Le CERTA recommande donc de mettre en œuvre diligemment les opérations de détection et de correction préconisées dans l'article du bulletin CERTA-2012-ACT-008.

Documentation

- Site du *DNS Changer Working Group* :
  http://www.dcwg.org
- Bulletin d'actualité du CERTA CERTA-2012-ACT-008 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2012-ACT-008/index.html
- Nombre d'adresses IP infectées par pays :
  http://www.dcwg.org/top-dns-changer-infections-by-country/

5 Rappel des avis émis

Dans la période du 29 juin au 05 juillet 2012, le CERTA a émis les publications suivantes :

- CERTA-2012-AVI-355 : Multiples vulnérabilités dans Symantec Message Filter
- CERTA-2012-AVI-356 : Multiples vulnérabilités dans Cisco WebEx Player
- CERTA-2012-AVI-357 : Multiples vulnérabilités dans IBM Rational ClearQuest
- CERTA-2012-AVI-358 : Multiples vulnérabilités dans HP System Management Homepage
- CERTA-2012-AVI-359 : Vulnérabilité dans des imprimantes HP Photosmart
- CERTA-2012-AVI-360 : Multiples vulnérabilités dans IBM Support Assistant
- CERTA-2012-AVI-361 : Multiples vulnérabilités dans WordPress
- CERTA-2012-AVI-362 : Vulnérabilité dans Network Node Manager I
- CERTA-2012-AVI-363 : Vulnérabilité dans Novell GroupWise
- CERTA-2012-AVI-364 : Vulnérabilité dans HP-UX
- CERTA-2012-AVI-365 : Vulnérabilité dans Avaya IP Office Customer Call Reporter
- CERTA-2012-AVI-366 : Vulnérabilité dans SPIP
- CERTA-2012-AVI-367 : Vulnérabilité dans TYPO3
- CERTA-2012-AVI-368 : Vulnérabilité dans RSA Access Manager

Durant la même période, la publication suivante a été mise à jour :

- CERTA-2012-AVI-344-001 : Vulnérabilités dans Joomla! (ajout références CVE)

6 Actions suggérées

6.1 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.

6.2 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.

6.3 Appliquer les correctifs de sécurité

Une faille connue publiquement et non-corrigée est une porte d'entrée sur un système d'information. Ce sont les cibles privilégiées des attaquants. Ils possèdent en effet tous les détails techniques nécessaires pour réaliser une exploitation de ces vulnérabilités. De nombreux malwares scannent également activement l'Internet à la recherche de ces failles. Il convient donc de corriger le plus rapidement possible les vulnérabilités signalées par les éditeurs.

6.4 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.

6.5 Analyser le réseau

Les codes malveillants peuvent également chercher à ouvrir des ports spécifiques ou à utiliser ceux ouverts par une compromission antérieure 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.

6.6 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 suspecte sur votre système d'information.

6.7 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/fr/anssi/formation/

Gestion détaillée du document

06 juillet 2012 version initiale.

10 juillet 2012 mise à jour de l'article « Décryptement des clés par des ressources PKCS#11 ».