Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 05 octobre 2012
N° CERTA-2012-ACT-040

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTA-2012-ACT-040

Gestion du document

Référence	CERTA-2012-ACT-040
Titre	Bulletin d'actualité CERTA-2012-ACT-040
Date de la première version	05 octobre 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 Révocation d'un certificat Adobe

Le 27 septembre 2012, *Adobe* a annoncé qu'une investigation était en cours concernant une utilisation frauduleuse d'un de ses certificats de signature de code. La cause serait due à la compromission d'un serveur de compilation de l'éditeur.

Ce certificat (*Adobe Systems Incorporated*) est signé par *VeriSign Class 3 Code Signing 2010 CA*, lui-même signé par *VeriSign Class 3 Public Primary Certification Authority - G5* :

- VeriSign Class 3 Public Primary Certification Authority - G5 (empreinte sha1 : `4E B6 D5 78 49 9B 1C CF 5F 58 1E AD 56 BE 3D 9B 67 44 A5 E5`, n de série : `18 DA D1 9E 26 7D E8 BB 4A 21 58 CD CC 6B 3B 4A`)
  - VeriSign Class 3 Code Signing 2010 CA (empreinte sha1 : `49 58 47 A9 31 87 CF B8 C7 1F 84 0C B7 B4 14 97 AD 95 C6 4F`, n de série : `52 00 E5 AA 25 56 FC 1A 86 ED 96 C9 D4 4B 33 C7`)
    - Adobe Systems Incorporated (empreinte sha1 : `FD F0 1D D3 F3 7C 66 AC 4C 77 9D 92 62 3C 77 81 4A 07 FE 4C`, n de série : `15 E5 AC 0A 48 70 63 71 8E 39 DA 52 30 1A 04 88`)

Plusieurs binaires potentiellement malveillants ont été retrouvés signés par ce certificat. L'un d'entre eux concerne l'utilitaire *PwDump* qui permet de récupérer des condensats de mots de passe d'un système Windows.
Les fichiers suivants ont été identifiés par *Adobe* comme potentiellement malveillants :

- `PwDump7.exe` (empreinte md5 : `130F7543D2360C40F8703D3898AFAC22`) ;

– `libeay32.dll` (empreinte md5 : `095AB1CCC827BE2F38620256A620F7A4`) ;
– `myGeeksmail.dll` (empreinte md5 : `46DB73375F05F09AC78EC3D940F3E61A`).

Le CERTA recommande d'effectuer une recherche de ces binaires sur les SI.

Ce certificat publié par *Adobe* est limité à la signature de code : il ne peut, par exemple, pas être utilisé dans le cadre de l'établissement d'une session SSL.

Sur un système *Windows Vista* ou *Windows 7* 64bits, la signature d'un pilote par ce certificat n'est pas une condition suffisante pour autoriser son chargement. En effet, il ne sera pas considéré comme valide, puisqu'il est nécessaire que ce fichier soit également contre-signé par *Microsoft*. Cependant, l'exécution d'un programme signé permet de contourner les restrictions de sécurité imposées par l'UAC sur les systèmes compatibles.

Adobe a demandé la révocation de ce certificat le 4 octobre 2012. Elle invalidera toutes les signatures émises par ce certificat depuis le 10 juillet 2012 et a été propagée automatiquement sur les postes connectés à l'Internet via une *CRL* (*Certificate Revocation List - Liste de révocation de certificats*) (cf. Documentation).

Sur certains systèmes, il peut être necessaire d'invalider le cache CRL afin de forcer une mise à jour en utilisant la commande suivante (avec les droits *administrateur*) :

```
certutil -setreg chain\ChainCacheResyncFiletime @now
```

L'impact de cette révocation sur un système est limité. En effet, seule l'installation (ou la réinstallation) d'applications signées avec ce certificat ne seront plus autorisées. Les applications *Adobe* déjà présentes, telles que *Flash Player*, seront considérées comme « non vérifiées », mais continueront à fonctionner correctement. Le CERTA recommande cependant de mettre à jour ces produits au plus vite. Une liste exhaustive de ces applications est disponible sur le site d'Adobe (cf. Documentation).

Des outils ont été publiés sur l'Internet permettant de rechercher les éventuels binaires signés par le certificat compromis. S'il est envisageable de les utiliser, ils doivent évidemment être testés avant d'être déployés sur un réseau en production.

Bien que significatif, cet incident ne peut être considéré avec la même gravité et les mêmes impacts que la compromission d'une autorité de certification telle que *Diginotar* l'année dernière. La mise à jour des certificats révoqués par l'intermédiare d'une liste de révocation n'ést pas un fait exceptionnel. Cependant, il doit conduire les responsables des SI à prendre en compte les contraintes imposées par une gestion des IGC sur les systèmes déconnectés.

Documentation

– Bulletin de sécurité Adobe apsa12-01 du 27 septembre 2012 :
`https://www.adobe.com/support/security/advisories/apsa12-01.html`
– Impacts sur les produits Adobe :
`http://helpx.adobe.com/x-productkb/global/certificate-updates.html`
– Article de bloc-notes Adobe du 27 septembre 2012 :
`http://blogs.adobe.com/asset/2012/09/inappropriate-use-of-adobe-code-signing-cert`
`html`
– Liste de révocation Verisign pour le certificat concerné :
`http://csc3-2010-crl.verisign.com/CSC3-2010.crl`

2 Windows invalide les certificats associés aux clés RSA inférieures à 1024 bits

Lors de la découverte en juin 2012 de certificats numériques usurpés utilisés pour tromper l'agent Windows Update (cf. CERTA-2012-ACT-023), Microsoft a reçu un sérieux signal sur l'importance des infrastructures de gestion de clés.

En réaction, l'éditeur a réalisé une première vague de durcissements de l'infrastructure Windows Update (notamment le client déployé sur les postes) dans le courant de l'été. Microsoft souhaite maintenant adresser plus largement les faiblesses des clés associées aux certificats utilisés dans l'industrie.

Le 20 juillet 2012, le CERTA publiait un article (CERTA-2012-ACT-029) relatif au renforcement par Microsoft de la validation des certificats sur la plate-forme Windows. Il s'agit notamment de la publication d'une mise à jour de Windows, invalidant les certificats utilisant des clés dont la taille est strictement inférieure à 1024 bits.

Cette mise à jour (kb2661254), disponible au téléchargement depuis cet été, sera déployée automatiquement par l'infrastructure Windows Update dès le 9 octobre prochain. Celle-ci est signalée par Windows Update comme

« critique » et « non liée à la sécurité » (à comprendre comme non liée à une correction de vulnérabilité). Il est communément répandu que les mises à jour critiques sont approuvées par les administrateurs Windows.

À partir du 9 octobre, nous allons donc assister à une brutale augmentation du déploiement de cette mise à jour, invalidant les certificats réputés faibles d'un point de vue cryptographique. Ainsi, les sites Internet accédés via SSL, les messages signés ou chiffrés pourront voir leur certificat associé évalué comme non valide par le système Windows, si leur clé RSA est d'une taille inférieure à 1024 bits. Désormais, les applications (navigateurs, clients mails, applications métier, ...) vont donc remonter à l'utilisateur l'usage d'un certificat dès lors invalide et, par exemple, bloquer l'accès à un service ou un site Internet. Des applications ou procédés automatiques peuvent également être affectés comme l'établissement de canaux VPN ou IPSec reposant sur des certificats invalidés.

Microsoft documente en détail comment identifier de tels certificats, ainsi que les moyens de déterminer les autorités de certification ayant émis des certificats faibles (cf. section documentation de cet article).

Le CERTA recommande donc une revue de l'usage des certificats dans votre environnement, afin de vous assurer qu'aucune application critique ne repose sur des certificats faibles. Si tel était le cas, le CERTA recommande de bloquer temporairement le déploiement de cette mise à jour et de procéder sans délai au renouvellement des certificats faibles pour de nouveaux certificats conformes aux recommandations du RGS.

Il est également important de signaler que la mise à jour sera déployée sans délai dans le grand public et qu'il conviendra donc d'accorder une attention immédiate aux services Internet proposés par les administrations, afin de s'assurer de leur utilisation de clés de chiffrement RSA supérieures à 1024 éléments binaires. Ceci afin d'en permettre un accès sans encombre par leurs utilisateurs.

Documentation

- Blocage des clés inférieures à 1024 éléments binaires :
  `http://blogs.technet.com/b/pki/archive/2012/06/12/rsa-keys-under-1024-bits-are-bloc`
  `aspx`
  `http://blogs.technet.com/b/pki/archive/2012/07/13/blocking-rsa-keys-less-than-102`
  `aspx`
  `http://blogs.technet.com/b/pki/archive/2012/08/14/blocking-rsa-keys-less-than-102`
  `aspx`
- Comment identifier si votre Autorité de Certificat Microsoft a émis des certificats dont les clés sont inférieures à 1024 éléments binaires :
  `http://blogs.technet.com/b/instan/archive/2012/08/03/how-to-identify-if-your-adcs`
  `aspx`
- Mise à jour concernant la longueur de clé minimale des certificats :
  `http://support.microsoft.com/kb/2661254`
- Bulletin d'actualité 2012-23 Article « Windows Update ou le retour de Flame » :
  `http://www.certa.ssi.gouv.fr/site/CERTA-2012-ACT-023/index.html`
- Article « Update to Windows Update, WSUS Coming This Week » :
  `http://blogs.technet.com/b/mu/archive/2012/06/06/update-to-windows-update-wsus-co`
  `aspx`
- Bulletin d'actualité 2012-029 Article « Renforcement de la politique de validation des certificats Microsoft » :
  `http://www.certa.ssi.gouv.fr/site/CERTA-2012-ACT-029/index.html`
- Profils de Certificats / LCR / OCSP et Algorithmes Cryptographiques :
  `http://www.ssi.gouv.fr/IMG/pdf/RGS_Profils_Certificat_LCR_OCSP_V2-3.pdf`

3 Gestion des données par un prestataire externe

L'entreprise Facebook a été récemment entendue par la CNIL suite aux plaintes de nombreux utilisateurs du réseau social. Ces utilisateurs auraient vu certains de leurs messages privés, destinés à d'autres utilisateurs de Facebook, rendus publics. Facebook a affirmé qu'il ne s'agissait pas d'un bogue, ce qui a été confirmé par la CNIL. L'incident est lié au nouveau mode de présentation du site. Le gouvernement a toutefois rappelé Facebook à l'ordre sur ses obligations en terme de protection des informations de ses utilisateurs.

Cet exemple illustre la problématique de la gestion des données par un prestataire externe. De nombreux services gratuits ou payants sont disponibles sur Internet comme les services de messagerie électronique (*webmail*), les relais de connexions par des serveurs mandataires (*proxies*), les réseaux sociaux, les services de stockage et de traitement dématérialisé d'informations (*Cloud computing*)...

L'utilisateur se sert de ces infrastructures pour stocker ou faire transiter ses informations et se repose sur elles pour en assurer la confidentialité et la disponibilité. Mais l'utilisateur doit être conscient qu'il prend le risque de perdre le contrôle de ses informations, ce qui est d'ailleurs parfois explicitement évoqué dans les conditions générales d'utilisation de ces services. Par ailleurs, l'utilisateur n'a aucun moyen de contrôle direct sur les éventuels mesures mises en œuvre pour assurer la confidentialité et la disponibilité de ses informations, et surtout aucune garantie sur leur devenir (modification du service, rachat de l'entreprise, sans consultation de l'utilisateur).

Le CERTA recommande de sensibiliser les utilisateurs sur les risques de transmission d'informations personnelles à des services non-maîtrisés et d'en interdire l'utilisation pour faire transiter ou stocker des données professionnelles.

Documentation

- Les conclusions de la CNIL sur le « bug » Facebook :
  `http://www.cnil.fr/la-cnil/actualite/article/article/les-conclusions-de-la-cnil-sur`
- Rappel à l'ordre du gouvernement :
  `http://proxy-pubminefi.diffusion.finances.gouv.fr/pub/document/18/13238.pdf`
- Guide pour maîtriser les risques de l'externalisation :
  `http://www.ssi.gouv.fr/fr/bonnes-pratiques/recommandations-et-guides/securite-de-l-externalisation/`

4 Discours du directeur général de l'ANSSI aux Assises de la sécurité 2012

Les Assises de la sécurité, qui se déroulent du 3 au 6 octobre 2012 à Monaco, ont été ouvertes par Patrick Pailloux, directeur général de l'ANSSI. Son discours d'introduction a mis l'accent sur :

- l'importance d'avoir une bonne hygiène informatique ;
- les risques liés à la mobilité ;
- la sécurité des systèmes industriels informatisés.

Ce discours est disponible sur le site de l'ANSSI (cf. documentation).

Documentation

- Discours du directeur général de l'ANSSI aux Assises de la sécurité 2012 :
  `http://www.ssi.gouv.fr/fr/anssi/publications/discours-de-patrick-pailloux-directeur-html`

5 Guide d'hygiène informatique

L'ANSSI a publié un guide d'hygiène informatique à destination des entreprises. Présenté sous forme d'appel à commentaires, ce guide propose quarante recommandations simples pour sécuriser un système d'information et protéger le patrimoine de l'entreprise.

Le CERTA recommande la lecture de ce guide et d'en appliquer les mesures proposées.

Documentation

- Guide d'hygiène informatique :
  `http://www.ssi.gouv.fr/IMG/pdf/Hygiene_informatique_20121002-1859.pdf`

6 Rappel des avis émis

Dans la période du 28 septembre au 04 octobre 2012, le CERTA a émis les publications suivantes :

- CERTA-2012-AVI-533 : Vulnérabilités dans Trend Micro Control Manager
- CERTA-2012-AVI-534 : Vulnérabilités dans IBM Rational Change
- CERTA-2012-AVI-535 : Vulnérabilités dans IBM RequisiteWeb
- CERTA-2012-AVI-536 : Vulnérabilité dans IBM Rational ClearQuest
- CERTA-2012-AVI-537 : Multiples vulnérabilités dans IBM Rational Synergy
- CERTA-2012-AVI-538 : Vulnérabilité dans IBM Rational Team Concert
- CERTA-2012-AVI-539 : Vulnérabilité dans IBM WebSphere Commerce
- CERTA-2012-AVI-540 : Vulnérabilité dans IBM AIX
- CERTA-2012-AVI-541 : Vulnérabilité dans Symantec Entreprise Vault product suite
- CERTA-2012-AVI-542 : Vulnérabilité dans HP IBRIX
- CERTA-2012-AVI-543 : Vulnérabilités dans CA License
- CERTA-2012-AVI-544 : Multiples vulnérabilités dans Citrix NetScaler SDX
- CERTA-2012-AVI-545 : Multiples vulnérabilités dans Wireshark

7 Actions suggérées

7.1 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.

7.2 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.

7.3 Appliquer les correctifs de sécurité

Le CERTA recommande l'application des correctifs de sécurité.

7.4 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.

7.5 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.

7.6 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.

7.7 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

05 octobre 2012 version initiale.