Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 08 juin 2012
N° CERTA-2012-ACT-023

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2012-23

Gestion du document

Référence	CERTA-2012-ACT-023
Titre	Bulletin d'actualité 2012-23
Date de la première version	08 juin 2012
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.

1 Facebook et DNSChanger

A l'instar de *Google* (voir bulletin d'actualité CERTA-2012-ACT-021), *Facebook* informe désormais ses utilisateurs de l'éventuelle infection de leur machine par *DNSChanger*. La notification affichée est alarmiste et contient un lien vers le site Web du *DNSChanger Working Group*.

Les risques sont les mêmes que ceux déjà énoncés dans le bulletin CERTA-2012-ACT-021 : des attaquants pourraient imiter ce genre de messages et insérer un lien vers un site Web malveillant.

Les recommandations restent les mêmes en cas d'apparition du message :

- en environnement professionnel, prévenir le RSSI ;
- pour les particuliers, confirmer une éventuelle infection en saisissant manuellement l'adresse du site Web du *DNSChanger Working Group*.

Documentation :

- Annonce du 4 juin 2012 sur le site de *Facebook* :
  https://www.facebook.com/notes/facebook-security/notifying-dnschanger-victims/10150833689760766
- Site Web du *DNSChanger Working Group* :
  http://www.dcwg.org/
- Bulletin d'actualité CERTA-2012-ACT-021 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2012-ACT-021/

2 Rappel sur les mots de passe

Suite à la publication, ces dernières semaines, de plusieurs millions de condensats de mots de passe exfiltrés de divers réseaux sociaux, le CERTA rappelle que des bonnes pratiques sont disponibles dans le document intitulé *Recommmandations de sécurité relatives aux mots de passe* (DAT-NT-001/ANSSI/SDE), sur le site Internet de l'ANSSI (section documentation). Elles comprennent notamment :

- la nécessité de différencier les mots de passe utilisés sur des systèmes d'information professionnels et des sites web publics (messagerie, réseaux sociaux, vente en ligne) ;
- le besoin d'utiliser un mot de passe complexe, voire non rejouable (*one time password*) ;
- le besoin de renouveler ces mots de passe avec une fréquence raisonnable ;
- ne pas configurer les logiciels pour se souvenir des mots de passe sensibles.

Le document présente également des méthodes d'attaque sur mots de passe dictant ces recommandations.

Enfin, il est rappelé aux autorités administratives que l'annexe B3 du référentiel général de sécurité (RGS) fixe l'ensemble des règles techniques à respecter en matière d'authentification.

Documentation :

- Recommandations de sécurité relatives aux mots de passe :
  `http://www.ssi.gouv.fr/IMG/pdf/NP_MDP_NoteTech.pdf`

3 Windows Update ou le retour de Flame

Flame est un code malveillant qui défraie actuellement l'actualité pour des raisons techniques et aussi géopolitiques. Le CERTA veut aujourd'hui se concentrer sur l'attaque réalisée sur le client Windows Update par ce code malveillant. En effet, Microsoft a publié cette semaine un avis de sécurité (2718704) révoquant trois certificats d'autorités intermédiaires utilisées dans le cadre de la distribution de licences Terminal Server.

L'avis CERTA-2012-AVI-304 du CERTA reprend cette information et recommande le déploiement de la mise à jour proposée. Le lendemain de cette publication exceptionnelle, Microsoft nous informe par le biais du blog MSRC que les « usurpations de contenu » et les « attaques d'interception » sont en réalité combinées par Flame pour parvenir à tromper l'agent Windows Update et déployer des mises à jour malveillantes. Ce supplément d'information change considérablement l'impact de cette vulnérabilité.

En effet, il est difficile de réaliser comment Microsoft a pu laisser créer ce lien entre la délivrance de licences Terminal Server et la chaine de confiance utilisée pour la mise à jour de la quasi-totalité du parc Microsoft Windows dans le monde.

Dans sa conception de l'agent Windows Update, Microsoft a choisi d'autoriser l'installation de toute mise à jour signée par un certificat issu d'une des trois autorités filles de `Microsoft Root Certificate Authority`.

Or, ces trois autorités intermédiaires utilisaient un algorithme faible pour les condensés (MD5) et autorisaient la délivrance de certificats pour la signature de code. Ces deux erreurs dans la création de ces autorités additionnées à une certaine légèreté des vérifications réalisées par l'agent Windows Update ont conduit à rendre vulnérable l'ensemble du système.

Ainsi, tout certificat valide, utilisable pour la signature de code, prétendant être émis par « Microsoft », pourra être utilisé pour contrefaire des mises à jour acceptables par l'agent Windows Update installé et activé par défaut par Microsoft sur l'ensemble du parc Windows client depuis Windows XP SP2. Il s'agit là d'une brèche importante dans le système de déploiement des mises à jour du parc Microsoft Windows, celui-là même dont toute la communauté sécurité encourage l'utilisation en pour pallier les vulnérabilités corrigées des produits Microsoft.

De plus, les analyses réalisées sur Flame laissent entendre que celui-ci circule sur Internet depuis deux ans : si cette information s'avérait exacte, cela signifierait que cette vulnérabilité est connue de certains attaquants de longue date et a pu être exploitée contre d'autres cibles, dans d'autres circonstances.

Au-delà de cet évènement malheureux, nous voici encore une fois devant un rappel cuisant : l'utilisation des outils basés sur la cryptographie (signatures, authentification, autorisation,...) n'apporte de réelle plus-value pour la sécurité qu'au travers d'une implémentation rigoureuse, au risque d'une illusion de sécurité.

Documentation :

- Avis du CERTA CERTA-2012-AVI-304 du 04 juin 2012 :
  `http://www.certa.ssi.gouv.fr/site/CERTA-2012-AVI-304/index.html`

– Bulletin Microsoft 2718704 du 03 juin 2012 :
http://technet.microsoft.com/en-us/security/advisory/2718704
– Articles du blog Microsoft Technet :
http://blogs.technet.com/b/srd/archive/2012/06/06/more-information-about-the-digita
aspx
http://blogs.technet.com/b/msrc/archive/2012/06/04/security-advisory-2718704-update
aspx

4 Rappel des avis émis

Dans la période du 01 au 07 juin 2012, le CERTA a émis les publications suivantes :
– CERTA-2012-AVI-300 : Vulnérabilité dans Cisco IOS XR
– CERTA-2012-AVI-301 : Vulnérabilité dans FreeBSD
– CERTA-2012-AVI-302 : Vulnérabilités dans les produits Horde
– CERTA-2012-AVI-303 : Vulnérabilité dans GIMP
– CERTA-2012-AVI-304 : Utilisation frauduleuse de certificats Microsoft
– CERTA-2012-AVI-305 : Vulnérabilité dans ISC BIND
– CERTA-2012-AVI-306 : Vulnérabilités dans Ruby on Rails
– CERTA-2012-AVI-307 : Vulnérabilités dans les produits Mozilla
– CERTA-2012-AVI-308 : Vulnérabilités dans Piwik
– CERTA-2012-AVI-309 : Vulnérabilité dans MIT Kerberos

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

– CERTA-2012-AVI-278-001 : Vulnérabilités dans Sympa (ajout de la référence CVE)

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

08 juin 2012 version initiale.