Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 01 juin 2012
N° CERTA-2012-ACT-022

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2012-22

Gestion du document

Référence	CERTA-2012-ACT-022
Titre	Bulletin d'actualité 2012-22
Date de la première version	01 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 Bonnes pratiques de préservation de traces suite à un incident

Le CERTA, dans le cadre d'analyse de compromissions, est parfois confronté à des supports de données où les informations ont été involontairement altérées. Ceci peut compliquer l'analyse, voire empêcher de retrouver des éléments importants pour la compréhension d'une compromission. C'est pourquoi la préservation d'un maximum de données est un aspect essentiel dans le cadre de la réponse à incident. Dans cette optique, voici quelques recommandations :

- éviter d'exécuter des outils de désinfection ou de nettoyage (anti-virus, défragmentation, etc.). Ceux-ci peuvent, par exemple, altérer l'historique visible des événements ou rendre plus difficile la récupération de données ;
- si possible, capturer une image de la mémoire avant d'éteindre la machine.

Pour de plus amples informations, vous trouverez dans la section *Documentation* un lien vers une note d'information du CERTA ainsi qu'un lien vers un article de recommendations de l'ICS-CERT qui est dans la même optique.

Documentation

- Article de recommandations concernant la réponse à incident de l'ICS-CERT :
  http://www.us-cert.gov/control_systems/pdf/ICS-TIP-12-146-01.pdf
- Note du CERTA sur les bons réflexes en cas d'intrusion sur un système d'information :
  http://www.certa.ssi.gouv.fr/site/CERTA-2002-INF-002/index.html

2 Chrome change sa manière de vérifier la validité des certificats

Les futures versions du navigateur *Chrome* n'utiliseront plus les méthodes usuelles de vérification de la validité des certificats, basées sur OCSP (*Online Certificate Status Protocol*) ou les CRL (*Certificate Revocation List*). Cette information a été annoncée en février 2012 par Adam Langley, un ingénieur logiciel travaillant chez *Google* et notamment sur *Chrome*.

Afin de comprendre les motivations derrière ce changement, voici un bref aperçu de l'utilisation des certificats dans le cadre des navigateurs Internet. Lorsqu'un navigateur se rend sur un site en HTTPS, il reçoit un certificat lui permettant de s'assurer qu'il se connecte bien au site souhaité. Dans ce certificat se trouvent également des pointeurs vers des services (CRL ou OCSP), en relation avec l'autorité de certification (AC) ayant signé le certificat. Ces services sont utilisés par les navigateurs pour déterminer si le certificat a été révoqué ou non. Le problème principal avec ce genre de vérification en ligne est que ces services peuvent devenir injoignables pour une quelconque raison. Dans ce cas, si les navigateurs exigeaient une réponse de ces services, la navigation serait momentanément impossible. Afin d'éviter ce cas de figure, lorsque une vérification de révocation en ligne échoue pour cause d'erreur réseau, la plupart des navigateurs ignorent simplement cette vérification de révocation (*soft-fail*). Les concepteurs de *Chrome*, non-satisfaits de ce système souhaitent arrêter son utilisation au sein de leur navigateur.

Comme méthode alternative, *Chrome* recevra des mises à jour logicielles incluant des listes de révocation de certificat. Bien que toujours sensible à la non-accessibilité temporaire des serveurs de mise à jour, cette méthode est jugée par ses promoteurs plus robuste car l'information de vérification sera disponible de manière anticipée, alors que dans le cas de la vérification de révocation en ligne, la tentative de communication avec les services de vérification est tentée seulement au fil de la navigation, lorsque cela est nécessaire. Par ailleurs, il revient maintenant à *Chrome*, à l'aide des AC, de maintenir à jour la liste des certificats révoqués à intégrer dans son navigateur. Néanmoins, une nouvelle problématique apparaît : les AC internes à des entreprises ne vont pas forcément communiquer leurs listes de révocation à *Google* et les services de révocation gérés par ces AC internes ne seront plus contactées par *Chrome*.

Documentation

– Article d'Adam Langley :
http://www.imperialviolet.org/2012/02/05/crlsets.html

3 Recommandations de sécurité relatives aux mots de passe

La note d'information CERTA-2005-INF-001 du CERTA *les mots de passe* est désormais intégrée au document *Recommandations de sécurité relatives aux mots de passe* disponible sur le site web de l'ANSSI (voir section Documentation).

Les recommandations minimales à respecter

A minima, l'ANSSI estime que les 8 recommandations suivantes doivent s'appliquer indépendamment de tout contexte. Lorsque les systèmes d'information utilisés le permettent, certaines doivent être imposées techniquement.

– Utilisez un mot de passe différent pour vous authentifier auprès de deux systèmes distincts. En particulier, l'utilisation d'un même mot de passe entre sa messagerie professionnelle et sa messagerie personnelle est impérativement à proscrire.
– Choisissez un mot de passe qui n'a pas de lien avec vous (mot de passe composé d'un nom de société, d'une date de naissance, etc.).
– Ne demandez jamais à un tiers de générer pour vous un mot de passe.
– Modifiez systématiquement et au plus tôt les mots de passe par défaut lorsque les systèmes en contiennent.
– Renouvelez vos mots de passe avec une fréquence raisonnable. Tous les 90 jours est un bon compromis pour les systèmes contenant des données sensibles.
– Ne stockez pas les mots de passe dans un fichier sur un poste informatique particulièrement exposé au risque (exemple: en ligne sur internet), encore moins sur un papier facilement accessible.
– Ne vous envoyez pas vos propres mots de passe sur votre messagerie personnelle.
– Configurez les logiciels, y compris votre navigateur web, pour qu'ils ne se « souviennent » pas des mots de passe choisis.

Documentation

- Recommandations de sécurité relatives aux mots de passe :
  http://www.ssi.gouv.fr/IMG/pdf/NP_MDP_NoteTech.pdf
- Les mots de passe :
  http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-001

4 Rappel des avis émis

Dans la période du 25 au 31 mai 2012, le CERTA a émis les publications suivantes :

- CERTA-2012-AVI-293 : Vulnérabilité dans IBM Lotus Quickr
- CERTA-2012-AVI-294 : Vulnérabilité dans Apache Commons Compress et Apache Ant
- CERTA-2012-AVI-295 : Multiples vulnérabilités dans Google Chrome
- CERTA-2012-AVI-296 : Vulnérabilité dans VMware
- CERTA-2012-AVI-297 : Multiples vulnérabilités dans EMC AutoStart
- CERTA-2012-AVI-298 : Vulnérabilités dans Asterisk
- CERTA-2012-AVI-299 : Vulnérabilité dans PyCrypto

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

01 mai 2012 version initiale.