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 août 2012
N° CERTA-2012-ACT-032

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : CERTA-2012-ACT-032

Conditions d'utilisation de ce document :	`http://www.certa.ssi.gouv.fr/certa/apropos.html`
Dernière version de ce document :	`http://www.certa.ssi.gouv.fr/site/CERTA-2012-ACT-032`

Gestion du document

Référence	CERTA-2012-ACT-032
Titre	CERTA-2012-ACT-032
Date de la première version	10 août 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.

Le bulletin d'actualité est disponible dans son intégralité et au format PDF à l'adresse suivante :
http://www.certa.ssi.gouv.fr/site/CERTA-2012-ACT-032.pdf
Un extrait du bulletin, ne reprenant que les articles de la semaine, se trouve en HTML à l'adresse suivante :
http://www.certa.ssi.gouv.fr/site/CERTA-2012-ACT-032/

1 Dangers liés à l'utilisation de MS-CHAPv2

MS-CHAPv2 est un protocole d'authentification conçu par Microsoft. Il a été introduit dans PPTP et peut être également utilisé dans WPA2 Entreprise.
Des attaques existent sur MS-CHAPv2 depuis au moins 1999. Plusieurs outils exploitant les faiblesses cryptographiques (comme l'utilisation du DES) ont été développés. En 2012, un nouvel outil, couplé à un service en ligne payant a été publié. Le temps nécessaire à la récupération des secrets d'authentification est considérablement réduit.

Les accès WiFi et VPN permettent généralement d'atteindre le réseau interne : ces services doivent reposer sur des protocoles d'authentification et de chiffrement éprouvés. En particulier, la conformité au RGS nécessite que la taille des clés symétriques utilisées jusqu'en 2020 soit au minimum de 100 bits, ce qui n'est pas le cas pour DES.

Les protocoles PPTP et WPA2 Entreprise utilisant l'authentification MS-CHAPv2 doivent exclusivement être employés dans un tunnel chiffré (ex. TLS). Ce tunnel doit garantir l'authenticité du serveur et la confidentialité de la communication.

Documentation

- Cryptanalysis of MS-CHAPv2 :
  http://www.schneier.com/paper-pptpv2.html
- Decipher MPPE by breaking MS-CHAPv2 :
  http://www.esec-pentest.sogeti.com/challenge-vpn-network/decipher-mppe-breaking-ms-chap-v2
- RGS v1, annexe B, mécanismes cryptographiques :
  http://www.ssi.gouv/fr/IMG/pdf/RGS_B_1.pdf

2 Flash dans le bac à sable

Il y a deux ans les équipes de Chrome, en collaboration avec Adobe, ont entamé la migration du plugin Flash dans l'architecture « Peeper Plugin API » de Google Chrome. Cette migration vient de s'achever, la version 21 de Google Chrome pour Windows intègre désormais la nouvelle monture du plugin d'Adobe. Cette version permet une amélioration de la sécurité en renforçant l'isolation du plugin Flash pour l'ensemble des versions de Windows. L'exécution du plugin Flash dans un « bac à sable » est une première pour les utilisateurs de Windows XP, qui se voient ainsi proposer une protection accrue de leur navigateur dans un système d'exploitation ne possédant pas les fonctionnalités de sécurité de Windows Vista ou Windows 7.

Le CERTA recommande donc aux utilisateurs de Google Chrome d'utiliser la version disposant de cette fonctionnalité.

Documentation

- The road to safer, more stable, and flashier Flash :
  http://blog.chromium.org/2012/08/the-road-to-safer-more-stable-and.html

3 Rappel des avis émis

Dans la période du 03 août 2012 au 09 août 2012, le CERTA a émis les publications suivantes :

- CERTA-2012-AVI-417 : Vulnérabilités dans Citrix Access Gateway
- CERTA-2012-AVI-418 : Vulnérablités dans IBM Eclipse Help System
- CERTA-2012-AVI-419 : Multiples vulnérabilités dans IBM AIX
- CERTA-2012-AVI-420 : Vulnérabilités dans Opera
- CERTA-2012-AVI-421 : Vulnérabilité dans Adobe Flash Player
- CERTA-2012-AVI-422 : Vulnérabilités dans LibreOffice
- CERTA-2012-AVI-423 : Vulnérabilité dans HP Network Node Manager I
- CERTA-2012-AVI-424 : Vulnérabilité dans Siemens Synco OZW
- CERTA-2012-AVI-425 : Vulnérabilité des drivers NVidia
- CERTA-2012-AVI-426 : Vulnérabilité dans EMC Iomega StorCenter

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

- CERTA-2012-AVI-084-001 : Vulnérabilités dans Adobe Flash Player (ajout de la tablette BlackBerry PlayBook dans les systèmes affectés)
- CERTA-2012-AVI-115-002 : Vulnérabilités dans Adobe Flash Player (ajout de la tablette BlackBerry PlayBook dans les systèmes affectés)
- CERTA-2012-AVI-176-001 : Vulnérabilités dans Adobe Flash Player (ajout de la tablette BlackBerry PlayBook dans les systèmes affectés)
- CERTA-2012-AVI-252-001 : Vulnérabilité dans Adobe Flash Player (ajout de la tablette BlackBerry PlayBook dans les systèmes affectés)

4 Actions suggérées

4.1 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.

4.2 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.

4.3 Appliquer les correctifs de sécurité

Le CERTA recommande l'application des correctifs de sécurité.

4.4 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.

4.5 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.

4.6 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.

4.7 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

10 août 2012 version initiale.