Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 06 janvier 2012
N° CERTA-2012-ACT-001

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2012-01

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-001

Gestion du document

Référence	CERTA-2012-ACT-001
Titre	Bulletin d'actualité 2012-01
Date de la première version	06 janvier 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-001.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-001/

1 Vulnérabilité de la semaine

1.1 Faiblesse dans le protocole *Wi-Fi Protected Setup* (WPS)

Un chercheur en sécurité a récemment révélé une faiblesse dans le protocole *Wi-Fi Protected Setup* (WPS) affectant la sécurité des points d'accès Wi-Fi supportant ce protocole. Malheureusement, la majorité des points d'accès Wi-Fi récents possèdent le WPS activé par défaut, ce qui touche une large gamme de produits.

1.1.1 Qu'est-ce que le WPS ?

Le but de WPS est de simplifier la configuration d'un client sans-fil. Les informations de sécurité (par exemple, la clé WPA2 dans le cas où ce protocole est utilisé) sont envoyées automatiquement au client par le point d'accès. Il y a trois modes possibles :

1. le mode *Push Button Connect* : il faut appuyer sur un bouton présent sur le point d'accès, ce qui lui permet de communiquer avec un client ayant besoin d'être configuré ;

2. le mode PIN client : l'appareil client possède un code PIN attribué par le fabriquant. Il faut alors se connecter à l'interface de configuration du point d'accès Wi-Fi et entrer le code PIN du client autorisé à récupérer les informations de configuration ;
3. le mode PIN routeur : le point d'accès Wi-Fi possède un code PIN secret de 8 chiffres qu'il faut renseigner sur un appareil client pour que ce dernier puisse récupérer les informations.

Les deux premières méthodes nécessitent un accès physique au point d'accès ou à son interface de configuration. En revanche, la troisième méthode nécessite seulement de connaître le code PIN secret de 8 chiffres et c'est dans celle-ci que se trouve la faiblesse.

En théorie, il existe cent millions de codes PIN possibles. Cependant, le protocole, tel qu'il est conçu, permet de trouver le bon code PIN en effectuant au maximum 11000 tentatives, ce qui rend les attaques par recherche exhaustive relativement efficaces.

Par conséquent, il est conseillé de désactiver le support du WPS lorsque celà est possible ou de mettre à jour le *firmware* du point d'accès Wi-Fi lorsque des mises à jour seront disponibles (se référer au constructeur de votre point d'accès).

Documentation

– Entrée du blog de Stephan Viehböck du 27 Décembre 2011 :
http://sviehb.wordpress.com/2011/12/27/wi-fi-protected-setup-pin-brute-force-vulnerability/

2 Incidents récents

2.1 Fuites de données sur des serveurs web

Le CERTA est régulièrement amené à contacter ses correspondants pour leur signaler des données accessibles à tous les internautes, alors que leur nature ne laisse pas supposer qu'une telle audience soit le fait d'un choix délibéré.

Dans certains cas, il s'agit de sauvegardes de la base de données situées dans l'arborescence des documents composant le site web.

Un site web construit sur une base de données est une situation courante. Les gestionnaires de contenu (CMS) comme Joomla!, SPIP, Drupal, etc... reposent sur une base de données pour produire les pages web à partir des articles et des canevas (*templates, skeleton...*). Ce contenu est public, en définitive, et l'accessibilité de ces sauvegardes peut ne pas choquer.

Le problème devient rapidement plus aigu avec les fonctions variées qu'offrent les CMS et qui permettent la manipulation de données nominatives ou de données sensibles comme des mots de passe. Ces fonctions, dans le CMS ou dans des extensions, recouvrent la gestion des contacts, donc des données personnelles, l'envoi d'une revue électronique (*newsletter*) donc la collecte d'adresses électroniques, des agendas, des extranets, etc...

Pour éviter ces fuites d'informations, les pistes sont diverses :

– pour des données telles que des configurations et des sauvegardes, le positionnement des fichiers hors de l'arborescence des documents et des scripts du site web est préférable ;
– le contrôle des droits positionnés lors de l'installation des logiciels tels les CMS et leurs extensions, et la rectification si nécessaire ;
– le positionnement des droits au niveau du système de fichiers ne doit permettre que les accès indispensables, aux comptes nécessaires ;
– pour les fichiers dans l'arborescence du site web, des protections telles que les fichiers `.htaccess` d'Apache permettent de limiter les accès ;
– éventuellement chiffrer les données.

3 Rappel des avis émis

Dans la période du 30 décembre 2011 au 05 janvier 2012, le CERTA a émis les avis suivants :

– CERTA-2011-AVI-727 : Vulnérabilités dans l'implémentation ASPNet du Microsoft .NET Framework
– CERTA-2011-AVI-728 : Vulnérabilité dans PHP
– CERTA-2011-AVI-729 : Vulnérabilité dans Ruby
– CERTA-2011-AVI-730 : Vulnérabilité dans Apache Tomcat

– CERTA-2012-AVI-001 : Vulnérabilité dans Arkoon FAST360
– CERTA-2012-AVI-002 : Vulnérabilité dans WordPress
– CERTA-2012-AVI-003 : Multiples vulnérabilités dans Apache Struts

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 tableau 2 rappelle les avis du CERTA correspondant aux applications ou codes malveillants relatifs aux ports étudiés dans les sections précédentes.

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

06 janvier 2012 version initiale.