Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 20 janvier 2012
N° CERTA-2012-ACT-003

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2012-03

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-003`

Gestion du document

Référence	CERTA-2012-ACT-003
Titre	Bulletin d'actualité 2012-03
Date de la première version	20 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.

1 Diffusion publique de données d'authentification

Cette semaine, le CERTA a été informé de la publication sur un site Web public d'une base de données contenant notamment des adresses mèl, ainsi que des données d'authentification sous forme de condensats de mot de passe. Il semble que ces données proviennent de la compromission du site Web communautaire.

Le CERTA a de nouveau constaté que dans cette liste apparaissaient de nombreuses adresses de messagerie professionnelles. Il est envisageable qu'un attaquant se serve de ces données pour tenter de se connecter à d'autres services que le site compromis initialement, comme à des extranets professionnels, des messageries, des *webmail*, des réseaux sociaux,etc. Le risque d'accès illégitime à d'autres informations est donc important si l'utilisateur réemploie le même mot de passe pour se connecter par exemple à l'extranet ou à la messagerie de son entreprise ou administration.

Le CERTA rappelle donc les bonnes pratiques suivantes :

– ne pas utiliser d'adresse mèl professionnel pour accéder à des sites hors de ce périmètre professionnel ;
– utiliser des identifiants différents pour se connecter à des services différents.

Enfin, comme la publication de ce type de données révèle la compromission d'un système d'information, le CERTA rappelle les bons réflexes à avoir face à un incident de ce type, renseignés dans la note d'information CERTA-2002-INF-002.

Documentation

- http://www.certa.ssi.gouv.fr/site/CERTA-2002-INF-002/index.html
- http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-001/index.html

2 Rappel des avis émis

- CERTA-2011-AVI-027 : Vulnérabilités dans Moodle
- CERTA-2012-AVI-015 : Multiples vulnérabilités dans Bluecoat PolicyCenter
- CERTA-2012-AVI-016 : Vulnérabilité dans PowerDNS
- CERTA-2012-AVI-017 : Vulnérabilité dans Sumatra PDF
- CERTA-2012-AVI-018 : Multiples vulnérabilités dans FFmpeg
- CERTA-2012-AVI-019 : Vulnérabilité dans ISC DHCP
- CERTA-2012-AVI-020 : Vulnérabilités dans Wireshark
- CERTA-2012-AVI-021 : Vulnérabilités dans PHP
- CERTA-2012-AVI-022 : Vulnérabilités dans HP StorageWorks Modular Smart Array P2000 G3
- CERTA-2012-AVI-023 : Multiples vulnérabilités dans les produits IBM
- CERTA-2012-AVI-024 : Multiples vulnérabilités dans les produits Oracle
- CERTA-2012-AVI-025 : Vulnérabilité dans Apache Tomcat
- CERTA-2012-AVI-026 : Vulnérabilité dans le serveur HTTP Apache

3 Actions suggérées

3.1 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.

3.2 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.

3.3 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.

3.4 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.

3.5 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.

3.6 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.

3.7 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

20 janvier 2012 version initiale.