Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 27 juillet 2012
N° CERTA-2012-ACT-030

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : CERTA-2012-ACT-030

Gestion du document

Référence	CERTA-2012-ACT-030
Titre	CERTA-2012-ACT-030
Date de la première version	27 juillet 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-030.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-030/

1 Systèmes industriels et supervision par Internet

Le CERTA a pris contact avec un industriel français qui exposait une interface de supervision de ses systèmes industriels sur l'Internet sans authentification préalable. Bien que cette interface ne permettait, a priori, aucune opération sur le système industriel, l'exploitation d'une vulnérabilité sur celle-ci permettrait à un attaquant de modifier le système industriel.

Afin de limiter les actes de malveillance, il convient de ne pas exposer ces interfaces au public. En cas de réel besoin de supervision par Internet, le CERTA rappelle la nécessité de mettre en place des contrôles d'accès à ces systèmes. Il est notamment recommandé :

- d'autoriser seulement les accès depuis des adresses IP identifiées ;
- de mettre en place un système d'authentification adapté (exemple : utilisation d'un mot de passe robuste) ;
- de dédier un réseau à la surveillance, et n'autoriser son accès depuis l'extérieur que via une passerelle sécurisée (exemple : VPN).

Documentation

– Note d'information du CERTA CERTA-2005-INF-001 "Les mots de passe" :
http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-001/index.html

2 Dangers liés aux plateformes non officielles de distribution d'applications mobiles

Les systèmes d'exploitation des terminaux mobiles continuent d'être des cibles privilégiées pour les auteurs de codes malveillants. Une application usurpant *Skype* est apparue récemment sur une plateforme non officielle de distribution d'applications *Android*. Cette dernière a pour but d'envoyer des *SMS* vers des numéros surtaxés. D'autres applications similaires existent, elles peuvent se faire passer pour un programme d'installation *Flash* ou prétendre être des navigateurs Internet.

Le CERTA recommande l'installation d'applications provenant uniquement de plateformes officielles de distribution et seulement quand l'éditeur de l'application peut être vérifié. Lorsque cela est possible, il est également recommandé de vérifier les permissions demandées par l'application ainsi que leur adéquation avec les fonctionnalités annoncées.

3 Alerte de sécurité pour les produits Microsoft Exchange et Fast Search Server 2010

Le 25 juillet 2012, le CERTA a émis une alerte de sécurité concernant les produits *Microsoft Exchange* et *Fast Search Server 2010*. Elle affecte plus précisément les bibliothèques *Oracle Outside In* utilisées par le service de transcodage des documents. *Oracle* a corrigé cette vulnérabilité lors des mises à jour du mois de juillet. La vulnérabilité peut être provoquée par l'ouverture d'une pièce jointe au moyen de *WebReady Document Viewing*, un système de pré-visualisation sous *Outlook Web Access*. Un attaquant peut ainsi exécuter du code arbitraire côté serveur.

Le CERTA recommande de se référer aux avis de sécurité publiés par *Microsoft* pour limiter les risques liés à cette faille (cf section Documentation).

Documentation

– Alerte CERTA-2012-ALE-004 du 25 juillet 2012 :
http://www.certa.ssi.gouv.fr/site/CERTA-2012-ALE-004/index.html
– Bulletin de sécurité Oracle cpujul2012-392727 du 17 juillet 2012 :
http://www.oracle.com/technetwork/topics/security/cpujul2012-392727.html
– Avis de sécurité Microsoft 2737111 du 24 juillet 2012 :
http://technet.microsoft.com/fr-fr/security/advisory/2737111
http://technet.microsoft.com/en-us/security/advisory/2737111
– Article du blog *Security Research and Defense* de Microsoft
http://blogs.technet.com/b/srd/archive/2012/07/24/more-information-on-security-advisory-2737111.aspx

4 Rappel des avis émis

Dans la période du 20 juillet 2012 au 26 juillet 2012, le CERTA a émis les publications suivantes :

– CERTA-2012-ALE-004 : Vulnérabilité dans Microsoft Exchange et Fast Search Server 2010
– CERTA-2012-AVI-396 : Vulnérabilités dans Moodle
– CERTA-2012-AVI-397 : Vulnérabilité dans PHP
– CERTA-2012-AVI-398 : Multiples vulnérabilités dans Symantec Web Gateway
– CERTA-2012-AVI-399 : Vulnérabilités dans Symantec System Recovery 2011 et Backup Exec System Recovery 2010
– CERTA-2012-AVI-400 : Vulnérabilités dans Red Hat Certificate System v8
– CERTA-2012-AVI-401 : Vulnérabilités dans Wireshark

– CERTA-2012-AVI-402 : Vulnérabilités dans Siemens SIMATIC STEP et PCS
– CERTA-2012-AVI-403 : Vulnérabilité dans Bash
– CERTA-2012-AVI-404 : Multiples vulnérabilités dans Safari
– CERTA-2012-AVI-405 : Vulnérabilités dans ISC BIND
– CERTA-2012-AVI-406 : Vulnérabilités dans ISC DHCP

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

27 juillet 2012 version initiale.