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 juillet 2012
N° CERTA-2012-ACT-029

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2012-029

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-029`

Gestion du document

Référence	CERTA-2012-ACT-029
Titre	Bulletin d'actualité 2012-029
Date de la première version	20 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-029.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-029/

1 Renforcement de la politique de validation des certificats Microsoft

Microsoft a annoncé récemment qu'une mise à jour renforçant la validation des certificats allait être proposée et déployée par Windows Update au mois d'août. Celle-ci ajoutera une vérification lors de la validation de la chaîne de certificats. Si un des certificats RSA utilise une clé de moins de 1024 bits, il sera considéré comme non valide et une erreur sera renvoyée à l'utilisateur.

L'ensemble des mécanismes utilisant des certificats est impacté : de l'authentification des serveurs à la signature de composants ActiveX ou les mécanismes de messagerie sécurisée S/MIME.

Cette modification du comportement par défaut devrait permettre une diminution significative du nombre de certificats utilisant une taille de clé trop faible. En effet, la partie « mécanismes cryptographiques » du référentiel général de sécurité (RGS) mentionne que la taille minimale du module RSA est de 2048 bits pour une utilisation de devant pas dépasser 2020 (et 4096 au delà de 2020).

Enfin, les autorités de certification racines doivent, dans tous les cas, utiliser des clés RSA de 2048 bits minimum, comme spécifié dans le *Microsoft Root Certificate Program*.

Documentation

- *RSA keys under 1024 bits are blocked*
  http://blogs.technet.com/b/pki/archive/2012/06/12/rsa-keys-under-1024-bits-are-blocked.aspx
- Microsoft Root Certificate Program
  http://technet.microsoft.com/en-us/library/cc751157.aspx
- Mécanismes cryptographiques : Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques
  http://www.ssi.gouv.fr/IMG/pdf/RGS_B_1.pdf

2 Retour sur la vulnérabilité XML Core

La semaine dernière, Microsoft a publié un correctif concernant XML Core Services. Ce dernier ne concerne que les versions 3.0, 4.0 et 6.0 pour toutes les versions maintenues de Microsoft Windows. Cette vulnérabilité est activement exploitée et plusieurs preuves de faisabilités sont disponibles sur l'Internet.

La correction de la version 5.0 qui concerne Microsoft Office 2003 et 2007 sera publiée dans un prochain bulletin Microsoft. C'est pourquoi le CERTA a maintenu son alerte CERTA-2012-ALE-003.

Le CERTA recommande de mettre à jour les versions 3.0, 4.0 et 6.0 avec la mise à jour publiée par Microsoft et, pour la version 5.0 :

- appliquer le contournement bloquant le vecteur d'attaque (*Fix it* 50908) ;
- déployer *Enhanced Mitigation Experience Toolkit* (EMET) ;
- configurer *Internet Explorer* de manière à obtenir un avertissement avant d'exécuter *Active Scripting* ou désactiver *Active Scripting* dans les zones de sécurité Internet et Intranet Local.

Documentation

- Bulletin de sécurité Microsoft MS12-043 du 10 juillet 2012 :
  http://technet.microsoft.com/fr-fr/security/bulletin/MS12-043
  http://technet.microsoft.com/en-us/security/bulletin/MS12-043
- Base de connaissance Microsoft KB2722479 du 10 juillet 2012 :
  http://support.microsoft.com/kb/2722479
- Base de connaissance Microsoft KB269238 :
  http://support.microsoft.com/kb/269238
- Article de bloc-notes de Microsoft du 10 juillet 2012 :
  http://blog.technet.com/b/srd/archive/2012/07/10/msxml-5-steps-to-stay-protected.aspx
- Alerte CERTA CERTA-2012-ALE-003 du 14 juin 2012 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2012-ALE-003
- Alerte CERTA CERTA-2012-AVI-375 du 11 juillet 2012 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2012-AVI-375

3 Microsoft met en garde les utilisateurs de gadgets

Microsoft a diffusé récemment un correctif consistant à désactiver les gadgets de Windows. Les gadgets sont souvent vus comme des applications simples et ayant un impact limité sur le système par les utilisateurs. En réalité, ceux-ci utilisent du code *JavaScript* sans bénéficier des contraintes de sécurités appliquées dans un environnement tel que *Internet Explorer*. Les accès au système offerts à ces gadgets sont nombreux et, de ce fait, ils peuvent être une cible de choix pour les attaquants. L'éditeur propose, notamment dans le cadre d'une utilisation professionnelle, de désactiver cette technologie en publiant une solution simple à déployer (FixIt, Stratégie).

Documentation

- Avis de sécurité Microsoft (2719662) du 10 juillet 2012 :
  http://technet.microsoft.com/fr-fr/security/advisory/2719662
- Article 2719662 de la base de connaissances Microsoft :
  http://support.microsoft.com/kb/2719662

4 Correctifs Oracle

Oracle a publié cette semaine une mise à jour corrigeant soixante-dix sept vulnérabilités dans de nombreux produits Oracle. Certaines vulnérabilités peuvent être exploités à distance et permettent notament l'exécution de code arbitraire.

Le CERTA recommande l'application de ces mises à jour dès que possible

Documentation

– Avis CERTA-2012-AVI-393 du 18 juillet 2012 :
http://www.certa.ssi.gouv.fr/site/CERTA-2012-AVI-393/index.html

5 Publications de l'ANSSI

L'ANSSI a publié cette semaine une note technique présentant les recommandations de sécurité relatives à un système GNU/Linux. Cette note présente différentes bonnes pratiques permettant de sécuriser un système GNU/Linux.

Ces recommandations sont particulièrement utiles pour assurer un durcissement du système. Le CERTA recommande la lecture et l'étude de cette note afin de déterminer la faisabilité et l'impact sur les SI correspondants.

L'ANSSI a également publié cette semaine une méthodologie et un outil d'audit des permissions d'un Active Directory. Celui-ci doit être utilisé dans un cadre légal, maîtrisé et conforme à la PSSI applicable. Il est publié sous licence de logiciel libre CeCILLv2 sur la forge publique *GitHub*.

Documentation

– Recommandations de sécurité relatives à un système GNU/Linux :
http://www.ssi.gouv.fr/fr/bonnes-pratiques/recommandations-et-guides/securite-du-poste-de-travail-et-des-serveurs/systeme-d-exploitation-linux/recommandations-de-securite-relatives-a-un-systeme-gnu-linux.html
– Méthodologie et outils d'audit des permissions d'un Active Directory :
http://www.ssi.gouv.fr/fr/menu/actualites/methodologie-et-outils-d-audit-des-permissions-d-un-active-directory.html

6 Rappel des avis émis

Dans la période du 13 juillet 2012 au 19 juillet 2012, le CERTA a émis les publications suivantes :

– CERTA-2012-AVI-386 : Vulnérabilité dans Libpng
– CERTA-2012-AVI-387 : Multiples vulnérabilités dans VMware ESXi
– CERTA-2012-AVI-388 : Vulnérabilité dans GLPI
– CERTA-2012-AVI-389 : Vulnérabilité dans divers produits EMC
– CERTA-2012-AVI-390 : Vulnérabilité dans HP AssetManager
– CERTA-2012-AVI-391 : Vulnérabilités dans IBM WebSphere
– CERTA-2012-AVI-392 : Vulnérabilité dans libexif
– CERTA-2012-AVI-393 : Multiples vulnérabilités dans les produits Oracle
– CERTA-2012-AVI-394 : Multiples vulnérabilités dans Mozilla Firefox et Thunderbird
– CERTA-2012-AVI-395 : Vulnérabiltés dans HP Network Node Manager i

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

– CERTA-2012-ALE-003-002 : Vulnérabilité dans Microsoft XML Core Services (mise à jour de l'alerte concernant XML Core 50)
– CERTA-2012-AVI-305-001 : Vulnérabilité dans BIND (ajout de AIX Bind)

7 Actions suggérées

7.1 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.

7.2 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.

7.3 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.

7.4 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.

7.5 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.

7.6 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.

7.7 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

13 juillet 2012 version initiale.