Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 13 avril 2012
N° CERTA-2012-ACT-015

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2012-15

Gestion du document

Référence	CERTA-2012-ACT-015
Titre	Bulletin d'actualité 2012-15
Date de la première version	13 avril 2012
Date de la dernière version	–
Source	–
Pièce(s) jointe(s)	Aucune

TAB. 1 – *Gestion du document*

Une gestion de version détaillée se trouve à la fin de ce document.

1 Vulnérabilités et mises à jour

1.1 Mise à jour dans Samba

Le projet Samba a publié un correctif pour supprimer une vulnérabilité dont l'impact peut être grave. L'attaquant peut, sans être authentifié, exécuter à distance du code arbitraire avec les droits administrateur.

Les distributions Linux publient les mises à jour pour corriger cette vulnérabilité.

Le CERTA rappelle l'impérieuse nécessité d'appliquer les correctifs de sécurité dans les plus brefs délais et en conformité avec la PSSI. Le filtrage complémentaire du port 139 en périphérie du SI s'inscrit dans une démarche de défense en profondeur.

Documentation

– Avis du CERTA CERTA-2012-AVI-210 du 12 avril 2012 :
http://www.certa.ssi.gouv.fr/site/CERTA-2012-AVI-210

1.2 Mise à jour mensuelle Microsoft

L'éditeur Microsoft a émis le 10 avril 2012 six bulletins de sécurité pour des correctifs couvrant onze vulnérabilités :

– Internet Explorer présente quatre vulnérabilités en rapport avec la gestion des tentatives d'accès à des objets

détruits et une cinquième liée à l'impression de pages HTML. Ces vulnérabilités permettent à l'attaquant d'exécuter du code arbitraire avec les droits de l'utilisateur concerné ;
- la vérification des programmes exécutables signés avec Authenticode présente une vulnérabilité qui permet à un attaquant modifier un programme sans provoquer de rejet lors de la vérification de signature ;
- le *framework* .NET présente une faiblesse exploitable pour exécuter du code arbitraire ;
- Forefront Unified Access Gateway présente deux vulnérabilités. L'une permet à un utilisateur non authentifié de se connecter à l'interface Web. L'autre permet de tromper un utilisateur légitime sur l'identité du serveur sur lequel il est effectivement connecté ;
- le composant MSCOMCTL.OCX permet l'exécution de code arbitraire avec les droits de l'utilisateur connecté au moyen d'une page Web spécialement construite. Ce composant est présent dans plusieurs versions de MS-Office, SQL Server, BizTalk Server, Commerce Server, Visual FoxPro et dans la bibliothèque d'exécution Visual Basic 6 ;
- le convertisseur de fichiers au format Works (extension .wps) contient un défaut qui permet l'exécution de code arbitraire avec les droits de l'utilisateur qui opère la conversion du fichier. Le composant vulnérable est présent dans MS Works 9, dans MS Works 6-9 File Converter et dans MS-Office 2007 SP2.

Le CERTA recommande d'appliquer les correctifs de l'éditeur dès que possible et selon la PSSI.

Documentation

- Avis du CERTA CERTA-2012-AVI-202 du 11 avril 2012 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2012-AVI-202
- Avis du CERTA CERTA-2012-AVI-203 du 11 avril 2012 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2012-AVI-203
- Avis du CERTA CERTA-2012-AVI-204 du 11 avril 2012 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2012-AVI-204
- Avis du CERTA CERTA-2012-AVI-205 du 11 avril 2012 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2012-AVI-205
- Avis du CERTA CERTA-2012-AVI-206 du 11 avril 2012 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2012-AVI-206
- Avis du CERTA CERTA-2012-AVI-207 du 11 avril 2012 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2012-AVI-207

1.3 Mise à jour Adobe

L'éditeur Adobe a émis un correctif pour les lecteurs de documents PDF Adobe Acrobat et Reader. Toutes les plateformes sont concernées. Plusieurs vulnérabilités, permettant l'exécution de code arbitraire, sont ainsi corrigées :

- une possibilité de contournement des restrictions d'accès dans l'installeur ;
- une corruption de la mémoire en utilisant du Javascript ;
- un débordement d'entier provoqué par l'utilisation d'une police de caractères *True Type* spécialement construite.

L'éditeur ne maintient plus les versions 9.4.x d'Adobe Reader sous Linux. Pour ce système d'exploitation, la version de référence est désormais la version 9.5.1.

Le CERTA constate que les courriels contenant des pièces jointes piégées au format PDF sont nombreux. Beaucoup utilisent des ressorts de l'ingéniérie sociale pour inciter les utilisateurs à ouvrir les pièces jointes. Il est donc impératif d'appliquer les correctifs dans les plus brefs délais, dans le respect de la PSSI.

Documentation

- Avis du CERTA CERTA-2012-AVI-208 du 11 avril 2012 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2012-AVI-208

1.4 Alerte sur RDP

Le CERTA n'a pas encore constaté d'exploitation de la vulnérabilité affectant le traitement du protocole RDP (*Remote Desktop Protocol*) sur Windows, corrigée dès le 13 mars 2012. De ce fait, l'alerte est levée sur le site Web du CERTA.

Toutefois, le CERTA rappelle que la menace est toujours potentiellement présente et que la prudence reste de mise. Il est donc impératif d'appliquer le correctif, si cela n'a pas encore été fait. Dans une optique de défense en profondeur, il convient également de bloquer les flux RDP en périphérie des SI chaque fois que ce protocole ne doit pas franchir de frontières entre SI, ou être utilisé entre le SI et un réseau externe.

Documentation

- Alerte du CERTA CERTA-2012-ALE-002 du 14 mars 2012 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2012-ALE-002
- Avis du CERTA CERTA-2012-AVI-138 du 14 mars 2012:
  http://www.certa.ssi.gouv.fr/site/CERTA-2012-AVI-138

2 Rappel des avis émis

Dans la période du 06 au 12 avril 2012, le CERTA a émis les publications suivantes :

- CERTA-2012-AVI-195 : Vulnérabilité dans F5 FirePass
- CERTA-2012-AVI-196 : Vulnérabilité dans Juniper IVE
- CERTA-2012-AVI-197 : Multiples vulnérabilités dans Google Chrome
- CERTA-2012-AVI-198 : Vulnérabilités dans MySQL
- CERTA-2012-AVI-199 : Multiples vulnérabilités dans RealNetworks Helix
- CERTA-2012-AVI-200 : Vulnérabilité dans Ghostscript
- CERTA-2012-AVI-201 : Vulnérabilité dans phpMyAdmin
- CERTA-2012-AVI-202 : Vulnérabilités dans Internet Explorer
- CERTA-2012-AVI-203 : Vulnérabilité dans l'Authenticode Windows
- CERTA-2012-AVI-204 : Vulnérabilité dans le Framework NET
- CERTA-2012-AVI-205 : Vulnérabilités dans Forefront Unified Access Gateway
- CERTA-2012-AVI-206 : Vulnérabilité dans Windows Common Controls
- CERTA-2012-AVI-207 : Vulnérabilité dans Microsoft Office
- CERTA-2012-AVI-208 : Vulnérabilités dans Adobe Acrobat et Reader
- CERTA-2012-AVI-209 : Présence d'un virus dans certains commutateurs HP
- CERTA-2012-AVI-210 : Vulnérabilité dans Samba
- CERTA-2012-AVI-211 : Vulnérabilités dans RPM

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

- CERTA-2012-AVI-085-001 : Multiples vulnérabilités dans Oracle Java (ajout du correctif Apple)
- CERTA-2012-AVI-210-001 : Vulnérabilité dans Samba (ajout des références aux bulletins Mandriva et RedHat)

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

13 avril 2012 version initiale.