Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 23 mars 2012
N° CERTA-2012-ACT-012

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2012-12

Gestion du document

Référence	CERTA-2012-ACT-012
Titre	Bulletin d'actualité 2012-12
Date de la première version	23 mars 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 Vulnérabilités Microsoft RDP

Lors de la publication du bulletin de sécurité MS12-020, concernant deux vulnérabilités dans l'implémentation de RDP (*Remote Desktop Protocol*), Microsoft a annoncé qu'un code d'exploitation serait à prévoir dans les 30 jours.

Cette prévision se réalise, des outils d'exploitation commencent à apparaître. Ceux-ci permettent, pour l'instant, de provoquer un déni de service. Leurs auteurs continuent leurs efforts pour accéder à une exécution de code arbitraire à distance. Outre ces programmes publics, le CERTA considère que des codes potentiellement plus dangereux peuvent déjà circuler dans des communautés plus restreintes.

Devant l'aspect critique de cette vulnérabilité, le CERTA maintient l'alerte et rappelle que les correctifs sont efficaces pour s'en prémunir.

Le CERTA recommande donc de prendre connaissance de l'article publié par Microsoft concernant les moyens de renforcer la sécurité face à cette menace et d'appliquer les correctifs disponibles au plus vite.

Documentations

– Article de Microsoft proposant des moyens de renforcer la sécurité face à cette menace en attendant d'appliquer les correctifs :
http://blogs.technet.com/b/srd/archive/2012/03/13/cve-2012-0002-a-closer-look-at-ms12-020-s-critical-issue.aspx

– Documents publiés par le CERTA traitant de ces vulnérabilités :
http://www.certa.ssi.gouv.fr/site/CERTA-2012-ALE-002/index.html
http://www.certa.ssi.gouv.fr/site/CERTA-2012-AVI-138/index.html
http://www.certa.ssi.gouv.fr/site/CERTA-2012-ACT-011/index.html

2 Rappel des avis émis

Dans la période du 16 au 22 mars 2012, le CERTA a émis les publications suivantes :

– CERTA-2012-AVI-147 : Vulnérabilité dans OpenLDAP
– CERTA-2012-AVI-148 : Multiples vulnérabilités dans les équipements XEROX
– CERTA-2012-AVI-149 : Vulnérabilité dans Cisco Catalyst 6500 et 5500
– CERTA-2012-AVI-150 : Vulnérabilités dans Cisco ASA et ASASM
– CERTA-2012-AVI-151 : Multiples vulnérabilités dans VMware
– CERTA-2012-AVI-152 : Vulnérabilités dans Joomla!
– CERTA-2012-AVI-153 : Vulnérabilités dans Asterisk
– CERTA-2012-AVI-154 : Vulnérabilité dans IBM Tivoli Endpoint Manager
– CERTA-2012-AVI-155 : Multiples vulnérabilités dans Citrix Licensing Administration Console
– CERTA-2012-AVI-156 : Multiples vulnérabilités dans IBM HTTP Server
– CERTA-2012-AVI-157 : Multiples vulnérabilités dans VLC
– CERTA-2012-AVI-158 : Vulnérabilités dans Aruba Networks
– CERTA-2012-AVI-159 : Multiples vulnérabilités dans Dell PowerVaul ML6000
– CERTA-2012-AVI-160 : Vulnérabilité dans JBoss
– CERTA-2012-AVI-161 : Vulnérabilité dans Nginx
– CERTA-2012-AVI-162 : Multiples vulnérabilités dans RSA enVision
– CERTA-2012-AVI-163 : Multiples vulnérabilités dans Moodle
– CERTA-2012-AVI-164 : Vulnérabilité dans Libpng
– CERTA-2012-AVI-165 : Multiples vulnérabilités dans Citrix XenServer
– CERTA-2012-AVI-166 : Multiples vulnérabilités dans Novell ZENworks
– CERTA-2012-AVI-167 : Vulnérabilités dans GnuTLS
– CERTA-2012-AVI-168 : Vulnérabilité dans CA ARCserv Backup

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

23 mars 2012 version initiale.