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 avril 2012
N° CERTA-2012-ACT-017

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2012-17

Gestion du document

Référence	CERTA-2012-ACT-017
Titre	Bulletin d'actualité 2012-17
Date de la première version	27 avril 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 Vulnérabilité critique dans Oracle TNS

Le 17 avril 2012, *Oracle* a diffusé une suite de correctifs de sécurité concernant ses produits (voir avis CERTA-2012-AVI-220). Parmi les vulnérabilités évoquées par *Oracle*, une d'entre elles semble ne pas avoir été corrigée, contrairement à ce qui était suggéré par l'avis de sécurité. Le découvreur mentionné par *Oracle* de cette faille prétend que l'éditeur n'a en réalité pas appliqué le correctif aux versions existantes de ses produits, mais qu'il serait intégré dans de futures versions. Par ailleurs, les détails concernant cette vulnérabilité, considérée comme critique, ont été publiés.

Le prochain correctif cumulatif d'*Oracle* est prévu pour le 17 juillet 2012.

Le CERTA n'a, pour le moment, pas connaissance d'attaques portant sur cette vulnérabilité, ni de l'existence d'outils permettant une exploitation automatique. Dans l'attente de clarification de la part de l'éditeur, il peut être judicieux de filtrer le port 1521/tcp sur les pare-feux.

Documentation :

– Avis CERTA-2012-AVI-220 :
http://www.certa.ssi.gouv.fr/site/CERTA-2012-AVI-220/

2 Logiciels dérivés

Certains programmes populaires, comme par exemple le navigateur *Mozilla Firefox*, font parfois l'objet de dérivés (aussi appelés *forks*). L'objectif de ces derniers est d'améliorer les performances dans des configurations bien particulières, ou encore d'ajouter des fonctionnalités. Leur utilisation pose toutefois des problèmes de sécurité. En effet :

- les dérivés partagent une bonne partie du code avec le produit d'origine, ce qui signifie qu'ils héritent généralement des vulnérabilités. Ainsi, une faille affectant *Mozilla Firefox* est susceptible de concerner tous ses développements parallèles ;
- le produit dérivé peut également faire l'objet de vulnérabilités qui lui sont propres, liées au code qui n'est pas partagé ;
- la publication des correctifs de sécurité d'un dérivé se fait généralement en différé par rapport au produit d'origine, parfois plusieurs mois après.

À titre d'exemple, la vulnérabilité ayant la référence CVE-2011-3658 a été corrigée en décembre 2011 pour *Mozilla Firefox*. *Pale Moon*, un des nombreux dérivés de *Mozilla Firefox*, n'a adapté le correctif qu'en avril 2012. Ce retard peut entraîner des risques de sécurité pour l'utilisateur final.

Le CERTA recommande d'évaluer l'impact en termes de sécurité, avant d'opter pour l'utilisation d'un dérivé plutôt que son produit d'origine.

3 Rappel des avis émis

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

- CERTA-2012-AVI-223 : Vulnérabilités dans Xoops
- CERTA-2012-AVI-224 : Vulnérabilité dans OpenSSL
- CERTA-2012-AVI-225 : Multiples vulnératilités dans HP-UX
- CERTA-2012-AVI-226 : Vulnérabilité dans IBM Rational ClearQuest
- CERTA-2012-AVI-227 : Vulnérabilités dans SPIP
- CERTA-2012-AVI-228 : Multiples vulnérabilités dans WordPress
- CERTA-2012-AVI-229 : Multiples vulnérabilités dans Asterisk
- CERTA-2012-AVI-230 : Vulnérabilités dans WebCalendar
- CERTA-2012-AVI-231 : Vulnérabilité dans IBM Tivoli Directory Server
- CERTA-2012-AVI-232 : Vulnérabilité dans HP-UX
- CERTA-2012-AVI-233 : Vulnérabilités dans IBM Rational AppScan et Policy Tester
- CERTA-2012-AVI-234 : Multiples vulnérabilités dans Mozilla
- CERTA-2012-AVI-235 : Multiples vulnérabilités dans Firefox Mobile

4 Actions suggérées

4.1 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.

4.2 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.

4.3 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.

4.4 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.

4.5 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.

4.6 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.

4.7 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 avril 2012 version initiale.