Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 30 mars 2012
N° CERTA-2012-ACT-013

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2012-13

Gestion du document

Référence	CERTA-2012-ACT-013
Titre	Bulletin d'actualité 2012-13
Date de la première version	30 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 Injection SQL : plus loin que l'extraction de données

1.1 Description

Les injections SQL et leurs tentatives font désormais partie du quotidien. Le CERTA est souvent amené à traiter des fuites d'informations, régulièrement obtenues par ce moyen.

Réduire l'impact des injections SQL à de l'exfiltration de données est une grave erreur. La vulnérabilité du système peut autoriser la modification, l'ajout ou la suppression de contenu. La modification peut se traduire par des défigurations partielles ou des messages revendicatifs sur des sites Web construits avec des CMS (*Content Management System*) qui s'appuyent sur des bases de données.

L'injection SQL ouvre aussi la porte à l'exécution de code à distance. En effet, le langage SQL permet de collationner un résultat de recherche dans un fichier. Cette fonction très utile peut être également utilisée par des attaquants. Il est ainsi possible de créer un fichier qui soit un interpréteur de commandes minimal écrit en PHP. L'attaquant dispose alors d'une porte dérobée sur le système.

Ce scénario catastrophe nécessite une vulnérabilité de type injection SQL ainsi qu'une configuration laxiste des permissions de PHP et des permissions sur les répertoires.

1.2 Recommandations

Face à cette menace, le CERTA recommande :

– de privilégier les procédures stockées dans les bases de données ;

– de développer les applications Web de manière rigoureuse pour éviter les vulnérabilités de type injection SQL. Par exemple, le filtrage systématique des entrées est indispensable ;
– d'auditer l'application et de faire des tests de pénétration avant mise en production ;
– de mettre à jour les systèmes et les logiciels ;
– de limiter les droits en écriture sur les répertoires au minimum indispensable ;
– de limiter les droits sur les opérations de la base de données, dont FILE, aux seuls utilisateurs pour lesquels ils sont nécessaires ;
– d'exécuter les processus avec les privilèges les moins élevés possible. Ceci est en particulier important pour les processus du serveur Web, de l'interprète PHP, du gestionnaire de base de données ;
– d'utiliser des dispositifs de filtrage en amont (*reverse proxy*, WAF) ;
– de journaliser l'activité et d'exploiter les journaux très régulièrement, l'idéal pour la réactivité étant une supervision au fil de l'eau ;
– de remplacer les comptes et les mots de passe par défaut et d'utiliser des mots de passe longs et complexes.

1.3 Documentation

– Note d'information du CERTA du 13 decembre 2004 sur les vulnérabilitées de type "Injection de données" http://www.certa.ssi.gouv.fr/site/CERTA-2004-INF-001/index.html
– Note d'information du CERTA du 20 mas 2007 sur l'utilisation de PHP : http://www.certa.ssi.gouv.fr/site/CERTA-2007-INF-002/index.html
– Note d'information du CERTA du 15 mars 2005 sur les mots de passe : http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-001/index.html
– Bulletin d'actualité du CERTA 2011-45 http://www.certa.ssi.gouv.fr/site/CERTA-2011-ACT-045/index.html
– Bulletin d'actualité du CERTA 2011-46 http://www.certa.ssi.gouv.fr/site/CERTA-2011-ACT-046/index.html

2 Google Play sur Samsung - Mise en garde

Certains utilisateurs d'ordiphone Samsung ont eu la surprise de voir s'installer sur leur mobile une application Russe. Cette application ne semble pas malveillante. Il s'avère que cette installation provient d'un dysfonctionnement de *Play Store (Android Market)*. En effet la vérification des mises à jour est faite par le nom des applications. L'application Russe porte le même nom que le logiciel de réception de courriel de Samsung. Ainsi, lors de sa mise à jour, c'est l'application Russe qui était téléchargée. Nous avons ici, en évidence, une faiblesse dans le processus de mise à jour de *Google Play Store*.

3 Mises à jour Adobe Flash Player automatiques

Aujourd'hui de nombreux logiciels malveillants se propagent via des logiciels *Adobe Flash Player* non mis à jour. Un des problèmes de l'obsolescense des versions se situe dans la procédure de mise à jour. En effet, dès lors qu'une mise à jour d'*Adobe Flash Player* est disponible, l'utilisateur doit manuellement accepter la mise à jour et l'installer. Ces actions ne sont malheureusement pas toujours effectuées. Lors de sa denière mise à jour, *Adobe Flash Player 11.2* proposera aux utilisateurs d'installer les mises à jour de façon automatique. Ce mécanisme vérifie la disponibilité d'une nouvelle version toutes les 24 heures. Le CERTA recommande d'effectuer cette dernière mise à jour et d'activer l'option d'installation automatique.

4 Rappel des avis émis

Dans la période du 23 au 29 mars 2012, le CERTA a émis les publications suivantes :

– CERTA-2012-AVI-170 : Multiples vulnérabilités dans Chrome
– CERTA-2012-AVI-171 : Multiples vulnérabilités dans IBM AIX
– CERTA-2012-AVI-172 : Vulnérabilités dans MediaWiki
– CERTA-2012-AVI-173 : Vulnérabilité dans Apache Traffic Server

– CERTA-2012-AVI-174 : Vulnérabilité dans eZ Publish
– CERTA-2012-AVI-175 : Multiples vulnérabilités dans Opera
– CERTA-2012-AVI-176 : Vulnérabilités dans Adobe Flash Player
– CERTA-2012-AVI-177 : Multiples vulnérabilités dans Cisco IOS Software
– CERTA-2012-AVI-178 : Vulnérabilité dans HP Performance Manager
– CERTA-2012-AVI-179 : Multiples vulnérabilités dans Novell iManager
– CERTA-2012-AVI-180 : Vulnérabilités dans Joomla!

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

– CERTA-2012-AVI-169-001 : Vulnérabilité dans OpenOffice LibreOffice (ajout du bulletin de sécurité LibreOffice)

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

23 mars 2012 version initiale.