

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2011-46

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-2011-ACT-046>

Gestion du document

Référence	CERTA-2011-ACT-046
Titre	Bulletin d'actualité 2011-46
Date de la première version	18 novembre 2011
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-2011-ACT-046.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-2011-ACT-046/>

1 Se prémunir contre les injections SQL

Dans le bulletin d'actualité 2011-45, nous avons brièvement présenté les vulnérabilités de type injection SQL, ainsi que des méthodes pour déterminer si un serveur web a été la cible d'attaque de ce type. Nous allons maintenant nous intéresser à des techniques à déployer en amont, lors du développement de l'application web, pour éviter d'être vulnérable à ce type d'attaque :

- se connecter à la base de données avec un compte aux privilèges limités ;
- vérifier que les données entrées par un utilisateur sont du type et du format attendu (longueur, intervalle de valeur). Par exemple, en PHP une fonction `is_numeric()` pour vérifier qu'une variable est bien de type numérique ;
- utiliser des fonctions spécifiques à une base de données pour « échapper » les caractères spéciaux dans une chaîne de caractère. Par exemple, nous trouvons en PHP `mysql_real_escape_string` ou `sqlite_escape_string()`. Lorsque les mécanismes d'échappement de caractères propres à une base de données ne sont pas disponibles, il est toujours possible d'utiliser `addslashes()` ou `str_replace()` ;

- utiliser des requêtes préparées (*prepared statement*). Cela consiste à créer un modèle de requête, en laissant des paramètres qui seront complétés ultérieurement. Une fois le modèle créé, il est possible de l'appeler en lui passant des arguments permettant de compléter la requête avant de l'exécuter. Un des avantages du point de vue de la sécurité réside dans le fait que les valeurs des paramètres sont automatiquement échappées si nécessaire.

Il est également possible de se protéger en mettant en place un *Web Application Firewall* (WAF) chargé d'inspecter les requêtes HTTP avant que le serveur web ne les traite, c'est le principe de la défense en profondeur. Cependant il est conseillé d'appliquer des bonnes pratiques de programmation et ne pas se reposer uniquement sur les fonctionnalités de filtrage d'un WAF.

De plus, le CERTA recommande une inspection régulière des journaux afin de détecter toute anomalie.

2 Rappel des avis émis

Dans la période du 11 au 17 novembre 2011, le CERTA a émis les publications suivantes :

- CERTA-2011-AVI-627 : Vulnérabilité dans *DB2 Query Monitor Tool*
- CERTA-2011-AVI-628 : Multiples vulnérabilités dans l'hyperviseur Xen
- CERTA-2011-AVI-629 : Vulnérabilités dans Novell ZENworks
- CERTA-2011-AVI-630 : Multiples vulnérabilités dans Adobe Flash Player
- CERTA-2011-AVI-631 : Vulnérabilités dans HP Network Node Manager i
- CERTA-2011-AVI-632 : Vulnérabilité dans GnuTLS
- CERTA-2011-AVI-633 : Vulnérabilité dans Juniper
- CERTA-2011-AVI-634 : Vulnérabilités dans Apple iOS
- CERTA-2011-AVI-636 : Vulnérabilité dans HP StorageWorks P4000 Virtual SAN Appliance
- CERTA-2011-AVI-637 : Vulnérabilité dans les produits Apple *Time Capsule* et *AirPort Base Station*
- CERTA-2011-AVI-638 : Vulnérabilités dans des produits Cisco TelePresence et Tandberg
- CERTA-2011-AVI-639 : Vulnérabilités dans HP OpenVMS
- CERTA-2011-AVI-640 : Vulnérabilités dans Joomla!
- CERTA-2011-AVI-641 : HP Directories Support for ProLiant Management Processors
- CERTA-2011-AVI-642 : Vulnérabilités dans Google Chrome
- CERTA-2011-AVI-643 : Vulnérabilité dans phpMyAdmin
- CERTA-2011-AVI-644 : Vulnérabilité dans AIX
- CERTA-2011-AVI-645 : Vulnérabilité dans ISC BIND

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

- CERTA-2011-AVI-635-001 : Vulnérabilité dans ProFTPD (ajout de la référence CVE et du bulletin de sécurité Debian)

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 réglementaire, 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 inexplicables 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

18 novembre 2011 version initiale.