

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2011-45

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-045>

Gestion du document

Référence	CERTA-2011-ACT-045
Titre	Bulletin d'actualité 2011-45
Date de la première version	10 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-045.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-045/>

1 Outils d'injection SQL automatique

Le CERTA constate de nombreuses tentatives et des réussites dans les attaques par injection SQL. Cet article présente le principe des outils et des motifs permettant de déceler ces attaques et ces tentatives.

1.1 Principe d'une injection SQL

Le langage SQL (*Structured Query Language*) est un langage utilisé pour manipuler les bases de données. Le principe est d'envoyer une requête SQL à un système de gestion de base de données (SGBD), ce qui permet d'extraire, d'ajouter, de modifier ou de supprimer des données dans la base de données.

Une application web, comme un serveur web doté d'un interpréteur PHP, utilise parfois une base de données pour fonctionner. Lorsque la manipulation de la base de données est effectuée à l'aide d'une requête SQL construite avec des données entrées par un utilisateur et que ces données ne sont pas vérifiées correctement, l'application web est potentiellement vulnérable à une attaque de type injection SQL.

Une attaque de type injection SQL consiste à fournir en paramètre d'une requête HTTP des données qui, une fois intégrées dans la requête SQL, seront interprétées par le SGBD et auront pour conséquence de construire

une requête malveillante. La requête SQL aura ainsi, sur la base de données, un effet autre que celui attendu par l'auteur de l'application web.

- Une telle faille peut être exploitée à plusieurs fins dont voici une liste non exhaustive :
- extraction, ajout, modification, suppression d'informations dans la base de données ;
 - exécution de code arbitraire à distance ;
 - élévation de privilèges ;
 - lecture de fichiers.

1.2 Outils automatisant l'exploitation d'une injection SQL

De nombreux sites sont la cible d'outils cherchant à exploiter de façon automatique des vulnérabilités de type injection SQL. L'utilisation la plus simple de ce type d'outil consiste généralement à entrer une URI vulnérable et laisser le programme trouver comment l'exploiter en laissant les paramètres par défaut. Cependant, pour des cas moins évidents à exploiter, il est souvent possible de paramétrer l'outil manuellement.

Détection d'un scan d'un outil d'injection SQL automatique

Il existe quelques moyens simples pour tenter de déterminer si un site a été la cible d'un outil d'injection SQL automatique. Ainsi en inspectant les journaux d'un serveur web, certaines caractéristiques peuvent alerter :

- certains outils, avec les paramètres par défaut, ajoutent une valeur spécifique dans l'en-tête HTTP `User-Agent` ;
- un nombre de requêtes HTTP par seconde anormalement élevé venant d'une même source ;
- des variables entrées par les utilisateurs prenant des valeurs suspectes (les journaux d'un serveur web enregistrent souvent l'URI demandée par l'utilisateur où, dans le cas d'une requête GET, des variables entrées par les utilisateurs apparaissent).

Voici un format typique d'une ligne suspecte apparaissant dans un journal de serveur web :

```
<ip_source> - - <date_et_heure> "GET /uri/vulnerable.php?Submit=Submit&id=999999.9%27+union+all+select+<...>2C0x31303235343830303536+and+%27x%273D%27x HTTP/1.1" 200 4567 "-" <User-Agent_suspect>
```

Ici deux caractéristiques peuvent attirer notre attention :

- la variable `id` possède une valeur suspecte, où l'on voit notamment des commandes SQL (`union`, `select`, etc.) ;
- le `User Agent` a un nom caractérisant un outil d'injection SQL automatique.

1.3 Documentation

- Note d'information du CERTA sur la sécurité des applications Web :
<http://www.certa.ssi.gouv.fr/site/CERTA-2004-INF-001/index.html>

2 Mise à jour Microsoft du mois de novembre et alerte

Cette semaine, Microsoft a publié quatre bulletins de sécurité pour ses produits. Parmi ces bulletins, deux traitent de vulnérabilités permettant de l'exécution de code arbitraire à distance. Une vulnérabilité dans la pile TCP/IP de Windows est considérée comme critique.

Il est important de noter qu'aucun de ces bulletins ne corrige la vulnérabilité mentionnée dans l'alerte CERTA-2011-ALE-006 publiée la semaine dernière. Le CERTA recommande donc le maintien du contournement provisoire, proposé par Microsoft, en attendant que cette vulnérabilité soit corrigée ; sous réserve de test avant déploiement.

Documentation

- Synthèse des bulletins de sécurité Microsoft de novembre 2011 :
<http://www.microsoft.com/fr-fr/security/bulletin/ms11-nov>

3 Sortie de la version 8 de Firefox

La nouvelle version du navigateur Web de la fondation *Mozilla* a été publiée le 08 novembre 2011. Elle apporte un certain nombre d'améliorations au niveau de la sécurité ainsi que différents correctifs.

Parmi les vulnérabilités corrigées, certaines, jugées critiques par l'éditeur, autorisent une exécution de code arbitraire à distance. Il est donc important d'effectuer la migration vers cette nouvelle version au plus vite.

La gestion des modules complémentaires (*add-ons*) a, elle aussi, été revue. Tout module de ce type ayant été installé par des programmes tiers est désormais désactivé jusqu'à la validation explicite de l'installation par l'utilisateur. Une fenêtre permettant la désactivation des modules déjà installés est aussi présentée à l'utilisateur lors de la mise à jour. Ces différentes mesures devraient permettre une meilleure gestion des *add-ons* par les utilisateurs et notamment empêcher l'installation d'extensions non désirées.

Documentation

- Bulletin de mise à jour Mozilla :
<https://www.mozilla.org/en-US/firefox/8.0/releasenotes/>
- Bulletins de sécurité Mozilla relatifs à Firefox :
<http://www.mozilla.org/security/known-vulnerabilities/firefox.html>

4 Rappel des avis émis

Dans la période du 04 au 10 novembre 2011, le CERTA a émis les publications suivantes :

- CERTA-2011-AVI-613 : Vulnérabilité dans les produits Cisco Small Business SRP500 Series
- CERTA-2011-AVI-614 : Vulnérabilité dans Novell Messenger
- CERTA-2011-AVI-615 : Vulnérabilité dans Squid
- CERTA-2011-AVI-616 : Vulnérabilités dans IBM AIX Bind
- CERTA-2011-AVI-617 : Vulnérabilité dans EMC Documentum eRoom
- CERTA-2011-AVI-618 : Vulnérabilités dans HP OpenView Network Node Manager
- CERTA-2011-AVI-619 : Vulnérabilité dans Juniper
- CERTA-2011-AVI-620 : Vulnérabilité dans RSA Key Manager Appliance
- CERTA-2011-AVI-621 : Vulnérabilité dans la pile TCP/IP de Windows
- CERTA-2011-AVI-622 : Vulnérabilité dans Microsoft Windows
- CERTA-2011-AVI-623 : Vulnérabilité dans Windows Mail et l'espace de collaboration Windows
- CERTA-2011-AVI-624 : Vulnérabilité dans Microsoft Active Directory
- CERTA-2011-AVI-625 : Multiples vulnérabilités dans Adobe Shockwave Player
- CERTA-2011-AVI-626 : Multiples vulnérabilités dans les produits Mozilla

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

- CERTA-2011-ALE-006-002 : Exploitation d'une vulnérabilité dans la gestion des polices TrueType sur Windows (ajout de la référence CVE)

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 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.

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 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.

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

10 novembre 2011 version initiale.