Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 29 juillet 2011
N° CERTA-2011-ACT-030

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2011-30

Gestion du document

Référence	CERTA-2011-ACT-030
Titre	Bulletin d'actualité 2011-30
Date de la première version	29 juillet 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-030.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-030/

1 Incidents de la semaine

Injection massive d'iframe

Cette semaine, le CERTA a traité un nombre conséquent d'incidents concernant des sites basés sur le gestionnaire de contenu web *osCommerce*. En effet, une attaque massive consistant à injecter une balise *iframe* dans la section *title* des pages vulnérables a été constatée.

Cette injection avait pour objectif de forcer le visiteur d'une page compromise à aller télécharger un code malveillant après une série de redirections. Au final, ce sont cinq vulnérabilités différentes affectant divers navigateurs qui étaient testées afin de compromettre la machine.

Le CERTA recommande donc aux utilisateurs de cette solution web de porter une attention toute particulière à l'intégrité du code source des pages web de leurs sites. En cas de compromission, il est nécessaire de réinstaller le serveur et un CMS à jour sur la base d'une sauvegarde saine et de changer les identifiants d'administration.

2 Fin de vie de la branche 2 du projet phpMyAdmin

À la lecture de l'avis CERTA-2011-AVI-411, l'absence de référence à la branche 2 du logiciel phpMyAdmin n'a échappé à personne.

En effet, cette branche ne bénéficie plus du support de l'équipe du projet, comme cela a été annoncé le 12 juillet 2011. Elle repose sur des briques PHP et MySQL, elles-mêmes anciennes. La version 2.11.11.3 est donc la dernière de cette branche pour laquelle aucun correctif de sécurité ne sera désormais émis.

Le CERTA recommande vivement aux utilisateurs de phpMyAdmin ou de logiciels incluant cet outil de vérifier les versions qu'ils utilisent. La migration vers des branches bénéficiant d'un support est indispensable. Lors du traitement d'incidents sur des serveurs, le CERTA constate régulièrement des attaques et des tentatives d'exploitations de vulnérabilités de certains logiciels dont phpMyAdmin.

Cette migration de phpMyAdmin pourra impliquer celles de PHP et de MySQL.

Documentation

- Site de téléchargement du projet phpMyAdmin :
  http://www.phpMyAdmin.net/home_page/downloads.php
- Annonce de fin de vie par le projet phpMyAdmin du 12 juillet 2011 :
  http://www.phpMyAdmin.net/home_page/news.php
- Note d'information du CERTA sur les systèmes obsolètes :
  http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-003/

3 HMTL5 et base de données

3.1 Web Storage

La récente norme HTML5 apporte son lot de nouveautés par rapport aux versions antérieures. Il devient notamment possible de stocker directement des informations au niveau du client Web grâce à une technologie dénommée *Web Storage*.

Cette idée n'est pas tout à fait nouvelle puisqu'elle se rapproche de la notion de *cookie*. Elle en reprend d'ailleurs l'une des bases : il s'agit, ici aussi, de stocker des données sous la forme de couples clé/valeur. Bien entendu, il ne s'agit pas d'une simple extension du système de cookies mais plutôt d'une nouvelle approche offrant des capacités étendues et une plus grande souplesse d'utilisation.

D'un point de vue plus technique, elle offre la possibilité de stocker et d'accéder à des données dans une base locale grâce à l'utilisation d'un simple script.

Afin de fournir ce service, deux types de bases différents sont disponibles : *session storage* et *local storage*. Elles diffèrent par leur nature : les bases de type *session storage* sont volatiles au sens où elles ont une durée de vie limitée à celle de la page les contenant alors que les bases de type *local storage* sont persistantes et vont par exemple servir à stocker le profil de l'utilisateur. Elles présentent aussi une différence importante au niveau de leurs droits d'accès. En effet, les bases de type *local storage* sont accessibles depuis l'ensemble des pages présentant le même triplé protocole/domaine/port que la page les ayant créés. Par exemple, une base créée par `http://exemple.com/index.html` sera accessible par `http://exemple.com/access.html` mais pas par `https://exemple.com/access.html` (notez le HTTPS au lieu du HTTP). Par contre, les bases de type *session storage* ne sont accessibles que par la page les ayant créées.

D'autres mécanismes de sécurité et de contrôle d'accès sont bien entendu prévus dans la spécification. Il est par exemple envisagé de pouvoir bloquer l'accès à la base de données d'un domaine par une *iframe* incluse dans l'une de ces pages. Des mécanismes de listes blanches/listes noires pour l'accès aux bases sont aussi à l'étude.

Des recommandations sont par ailleurs émises concernant le contenu pouvant être mis en base. Il est, par exemple, déconseillé d'y stocker des mèls ou toutes sortes d'informations sensibles.

Cependant, il s'agit de recommandations présentes dans la spécification de la norme (qui est toujours en développement) et rien ne garantit que les différentes implémentations les suivront. De plus, aucun mécanisme ne permet de prévenir le stockage de données sensibles. Diverses attaques permettant de contourner les mécanismes de protections et d'accéder aux données stockées sont aussi envisageables (par exemple, par une usurpation de nom DNS). Il est donc nécessaire de rester vigilant et de prendre garde aux types de données que l'on souhaite inclure dans une base lors du développement d'un site utilisant ce type de technologies.

Actuellement, les versions majeures des navigateurs les plus populaires supportent cette norme.

3.2 Web SQL Database

Outre *Web storage*, différentes solutions de stockage ont été envisagées lors du développement de HTML5. *Web SQL Database* en est une. Son développement a cependant été abandonné au mois de novembre 2010. Il est tout de même intéressant de noter que certains navigateurs comportent une implémentation de ces mécanismes : *Google Chrome*, *Safari* et *Opera*.

Sans rentrer dans les détails, cette solution se rapproche des technologies employées dans les bases de données et interprètent directement sur le langage SQL. Elle comporte cependant les mêmes problématiques de sécurité et de protection de la vie privée que *Web storage*. À ce titre, il est, ici aussi, important de bien considérer les types d'informations que l'on va insérer dans cette base lors de son utilisation.

3.3 Documentation

- W3C Web Storage :
  http://dev.w3.org/html5/webstorage/
- W3C Web SQL DataBase :
  http://w3.org/TR/webdatabase/
- Dive into HTML5 :
  http://diveintohtml5.org/

4 Vulnérabilité dans Apple iOS liée à la validation de la chaîne de certificats X.509

Cette semaine Apple a publié une nouvelle mise à jour concernant iOS pour iPhone, iPod et iPad.

Une erreur lors de la vérification d'une extension d'un certificat X.509 (*Basic Constraints*) permet à un utilisateur malintentionné, en utilisant un certificat de fin de chaîne valide (donc non considéré comme autorité de certification), de signer un nouveau certificat dédié à un domaine quelconque et de le présenter comme valide. Lorsque celui-ci sera utilisé, aucun avertissement ne sera envoyé à l'utilisateur mentionnant que le certificat n'est pas valide.

Cette vulnérabilité peut être utilisée afin de réaliser des attaque de type «*man-in-the-middle*» et ainsi de récupérer et/ou modifier les informations transmises lorsque des transmissions HTTPS sont utilisées.

Le CERTA recommande d'appliquer la mise à jour dès que possible.

Documentation

- Avis CERTA-2011-AVI-412 du 26 juillet 2011 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2011-AVI-412/

5 Liens utiles

- Mémento sur les virus :
  http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-002/
- Note d'information du CERTA sur l'acquisition de correctifs :
  http://www.certa.ssi.gouv.fr/site/CERTA-2001-INF-004/
- Note d'information du CERTA sur les systèmes obsolètes :
  http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-003/
- Note d'information du CERTA sur les bonnes pratiques concernant l'hébergement mutualisé :
  http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-005/
- Note d'information du CERTA sur les mots de passe :
  http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-001/
- Note d'information sur la terminologie d'usage au CERTA :
  http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-002/
- Note d'information du CERTA sur les enjeux de sécurité liés à une migration vers IPv6 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-004/

- Unix security checklist version 2.0 du 8 octobre 2001 (Publication du CERT australien) : http://www.auscert.org.au/render.html?it=1937
- Note d'information du CERTA sur les risques associés aux clés USB : http://www.certa.ssi.gouv.fr/site/CERTA-2000-INF-006/
- Note d'information du CERTA sur les outils d'indexation et de recherche : http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-009/
- Note d'information du CERTA sur la gestion des noms de domaine : http://www.certa.ssi.gouv.fr/site/CERTA-2007-INF-001/
- Note d'information du CERTA sur le bon usage de PHP : http://www.certa.ssi.gouv.fr/site/CERTA-2007-INF-002/

6 Rappel des avis émis

Dans la période du 22 au 28 juillet 2011, le CERTA a émis les publications suivantes :

- CERTA-2011-AVI-409 : Vulnérabilités dans Foxit Reader
- CERTA-2011-AVI-410 : Vulnérabilités dans SquirrelMail
- CERTA-2011-AVI-411 : Vulnérabilités dans phpMyAdmin
- CERTA-2011-AVI-412 : Vulnérabilité dans Apple iOS
- CERTA-2011-AVI-413 : Vulnérabilités dans iWork
- CERTA-2011-AVI-414 : Vulnérabilités dans Nagios
- CERTA-2011-AVI-415 : Vulnérabilité dans ClamAV
- CERTA-2011-AVI-416 : Vulnérabilités dans Samba (SWAT)

7 Actions suggérées

7.1 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.

7.2 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.

7.3 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.

7.4 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.

7.5 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.

7.6 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.

7.7 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

8 Les bulletins d'actualité

L'objectif des *bulletins d'actualité* est de fournir une illustration par l'actualité récente de certaines mesures de sécurité pragmatiques à appliquer. Bien que par nature *a posteriori*, cette illustration a vocation à servir de base pour tirer des enseignements plus généraux à même de protéger contre des incidents futurs.

L'« actualité » est donnée par l'analyse de machines que le CERTA réalise dans le cadre de ses missions. Un fait est jugé d'actualité, s'il est à la fois récent et significatif, c'est à dire recoupé par différentes analyses.

Les *bulletins d'actualité* n'ont pas la prétention de constituer des statistiques fiables de l'activité informatique malveillante, mais ce qui nous semble avoir beaucoup plus d'intérêt, de montrer à partir d'exemples concrets, réels et anonymisés comment découvrir que l'on est ou a été attaqué et comment limiter l'impact de ces attaques.

La qualité des *bulletins d'actualité* sera améliorée grâce à votre participation. Si vous souhaitez participer, prenez contact avec le CERTA en accord avec votre chaîne fonctionnelle de la sécurité des systèmes d'information.

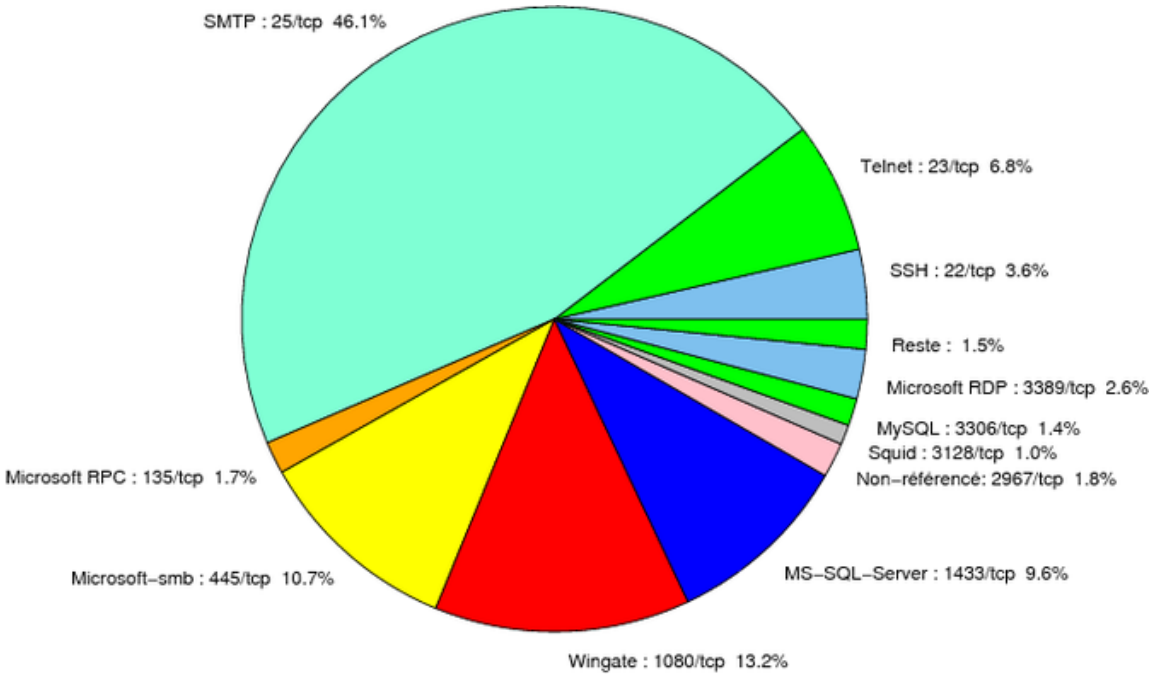

FIG. 1: Répartition relative des ports pour la semaine du 22 au 28 juillet 2011

port	pourcentage
25/tcp	46.08
1080/tcp	13.22
445/tcp	10.65
1433/tcp	9.62
23/tcp	6.8
80/tcp	5.77
22/tcp	3.59
3389/tcp	2.56
2967/tcp	1.79
135/tcp	1.66
3306/tcp	1.41
3128/tcp	1.02
4899/tcp	0.89
21/tcp	0.25
9898/tcp	0.12

TAB. 2: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

29 juillet 2011 version initiale.