

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2011-07

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-007>

Gestion du document

Référence	CERTA-2011-ACT-007
Titre	Bulletin d'actualité 2011-07
Date de la première version	18 février 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-007.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-007/>

1 Problématique de filtrage

Une entité souhaite souvent que son site Web soit le plus populaire possible. Pourtant, certains types de connexions peuvent ne pas être souhaitables, en particulier lorsque les utilisateurs ne se connectent pas de leur plein gré, mais que le contenu est inclus de manière illégitime dans d'autres sites. Par exemple, des sites de filoutage ou des sites diffamatoires peuvent inclure le contenu d'un site officiel, afin, dans le premier cas, de rendre l'attaque moins identifiable par l'utilisateur visé et dans le second cas, d'associer le site officiel à un contenu ou un nom de domaine qui n'est pas souhaité et qui peut porter préjudice.

Le contenu du site officiel peut être inclus de manières variées dans des sites illégitimes. En langage HTML, différentes balises peuvent être utilisées pour réaliser une inclusion de contenu : DIV, IFRAME ou FRAME. La suite de l'article indique comment s'en prémunir. Toutefois, la seconde parade proposée ne fonctionnera pas pour traiter les redirections (codes HTTP 301, 303 ou 307 ou balise HTML <META HTTP-EQUIV=' '>).

1.1 Filtrage sur la base du Referer

La première solution est de réaliser un filtrage basé sur le champ de l'entête HTTP Referer. L'entête Referer est transmise lorsqu'un utilisateur suit un lien, interne ou externe, pour préciser au site cible d'où

vient l'utilisateur. Ainsi, si un site malveillant fait une inclusion de contenu ou une redirection illégitime d'un site ciblé, ce dernier verra apparaître dans les requêtes qui lui sont adressées un entête `Referer` faisant référence au site illégitime. Il suffit alors de créer une règle de filtrage sur le serveur Web du site ciblé pour interdire ce genre de requête ou leur délivrer des réponses modifiées. Cela peut par exemple être mise en œuvre très facilement avec `mod_security` avec une règle telle que :

```
SecDefaultAction phase:1,deny
SecRule REQUEST_HEADERS:Referer 'site-malveillant.*'
```

Toutefois, ce filtrage devra être mis à jour à l'apparition de chaque nouveau site indésirable. Une procédure pourrait être mise en œuvre pour surveiller les journaux d'activité en vue d'identifier au fur et à mesure les valeurs de `Referer` à filtrer.

1.2 Utilisation de X-Frame-Options

L'entête HTTP `X-Frame-Options` peut être ajoutée pour indiquer au navigateur de l'utilisateur qu'il doit afficher un site Web lorsqu'il est inclus dans une balise HTML `FRAME` ou `IFRAME`. De plus, cette option offre une protection contre certaines attaques de type XSS.

Le support de cette option par les navigateurs est assez récent (Internet Explorer 8 à partir de janvier 2009, Firefox 3.6.9, Safari 4, chrome 4.1.249.1042).

La valeur de l'entête peut être `DENY`, pour interdire complètement les inclusions, ou `SAMEORIGIN`, pour n'autoriser que les inclusions en provenance d'une page du même domaine (plus précisément, le même *Fully Qualified Domain Name* : `FQDN`).

Sur un serveur Apache, l'entête `X-Frame-Options` peut être ajoutée avec la clause suivante dans la configuration :

```
Header always append X-Frame-Options SAMEORIGIN
```

1.3 Documentation

- Site officiel du pare-feu applicatif web `modsecurity` :
<http://www.modsecurity.org/>
- Documentation concernant l'option `X-Frame` :
<http://blogs.msdn.com/b/ieinternals/archive/2010/03/30/combatting-clickjacking-with-x-frame-options.aspx>
<http://blog.mozilla.com/security/2010/09/08/x-frame-options/>
http://www.owasp.org/index.php/Clickjacking#Defending_with_response_headers

2 TYPO3 v4.5 et nouvelles fonctionnalités

La version 4.5 de TYPO3 est disponible. Cette version ajoute une nouvelle fonctionnalité afin de protéger l'utilisateur contre des attaques de type injection de requêtes illégitimes par rebond (CSRF).

Présentée parfois comme un correctif, cette fonctionnalité ne sera présente qu'à partir de la version 4.5 de TYPO3. Une nouvelle API permet de protéger les formulaires de ce type d'attaque en imposant à certaines extensions du CMS de fournir un « jeton » unique. La protection apportée par l'API ne sera efficace que si les développeurs d'extensions l'utilisent.

Outre cette nouvelle fonctionnalité et afin de se protéger contre ce type d'attaque, le CERTA recommande de ne pas consulter en même temps et avec un même navigateur plusieurs sites dont certains contiendraient des données sensibles.

Documentation

- Note d'information CERTA-2008-INF-003 concernant les attaques de type « cross-site request forgery » :
<http://www.certa.ssi.gouv.fr/site/CERTA-2008-INF-003>
- Notes de la version 4.5 de TYPO3 :
<http://typo3.org/download/release-notes/typo3-45/>

- Nouvelles fonctionnalités concernant la sécurité de la version 4.5 de TYPO3 :
http://wiki.typo3.org/TYPO3_4.5#Security
<http://buzz.typo3.org/teams/security/article/typo3-45-will-be-the-most-secure-typo3-version-ever/>

3 Fin de vie de FreeBSD 7.1

Le projet FreeBSD qui produit le système d'exploitation éponyme tient à jour un tableau précis des cycles de vie de ses différentes versions encore maintenues. Ainsi, il est possible de trouver à l'adresse : <http://security.freebsd.org> les modalités de supports relatives à chaque branche du projet (7 et 8) ainsi que, pour chacune d'entre elles, les différentes versions et leur positionnement dans son cycle de vie.

On peut ainsi remarquer que la version 7.1 arrive, *a priori*, en fin de support étendu le 28 février prochain et devra être remplacée par, au minimum, la version 7.3 ou mieux par une version maintenue de la branche 8 (8.1 ou bientôt 8.2).

Recommandations :

Il conviendra de mettre à jour dans les plus brefs délais cette version si elle est encore déployée. Par ailleurs, il est à noter que, malgré une complexité plus importante, une migration vers les toutes dernières versions reste la démarche la plus avantageuse en matière de durée de vie et de richesse de fonctionnalités.

4 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/>

5 Rappel des avis émis

Dans la période du 11 au 17 février 2011, le CERTA a émis les avis suivants :

- CERTA-2011-AVI-085 : Vulnérabilité dans OpenSSH
- CERTA-2011-AVI-087 : Vulnérabilité dans Novell eDirectory
- CERTA-2011-AVI-088 : Vulnérabilité dans Novell iPrint

- CERTA-2011-AVI-089 : Multiples vulnérabilités dans les paquetages tiers pour VMware
- CERTA-2011-AVI-090 : Vulnérabilité dans F-Secure Internet Gatekeeper
- CERTA-2011-AVI-091 : Vulnérabilité dans phpMyAdmin
- CERTA-2011-AVI-092 : Multiples vulnérabilités dans OpenLDAP
- CERTA-2011-AVI-093 : Multiples vulnérabilités dans Oracle Java
- CERTA-2011-AVI-094 : Vulnérabilité dans shadow
- CERTA-2011-AVI-095 : Vulnérabilités dans Cisco SA Management Center

Durant la même période, les avis suivants ont été mis à jour :

- CERTA-2011-AVI-046-001 : Vulnérabilité dans VLC Media Player (ajout de la référence au bulletin Debian et des références CVE)
- CERTA-2011-AVI-070-001 : Multiples vulnérabilités dans Google Chrome (ajout des références CVE)
- CERTA-2011-AVI-073-001 : Vulnérabilité dans OpenSSL (ajout des références aux bulletins Fedora, Mandriva et Ubuntu)
- CERTA-2011-AVI-078-001 : Vulnérabilités dans MIT Kerberos (ajout des références aux bulletins RedHat et Ubuntu et rectification des CVE)
- CERTA-2011-AVI-079-001 : Vulnérabilité dans plusieurs implémentations de Java (ajout pour IBM Java, IBM WebSphere Application Server, et IBM Webspere Portal)
- CERTA-2011-AVI-086-001 : Multiples vulnérabilités dans Django (ajout de la référence au bulletin Debian et des références CVE)

6 Actions suggérées

6.1 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.

6.2 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.

6.3 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.

6.4 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.

6.5 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.

6.6 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.

6.7 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

Liste des tableaux

1	Gestion du document	1
---	-------------------------------	---

Gestion détaillée du document

18 février 2011 version initiale.