Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 17 juillet 2008
N° CERTA-2008-INF-001

Affaire suivie par :
CERTA

NOTE D'INFORMATION DU CERTA

Objet : iFRAME, fonctionnement et protection

Gestion du document

Référence	CERTA-2008-INF-001
Titre	iFRAME, fonctionnement et protection
Date de la première version	17 juillet 2008
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 Introduction

Parmi les méthodes de compromission rencontrées sur l'Internet et traitées par le CERTA dans le cadre de ses missions, il est de plus en plus courant de rencontrer l'insertion de balise *iFRAME* dans les codes sources des pages des sites web. Le but de cette note d'information est définir le principe de fonctionnement de ces *iFRAME* et les moyens pour les utilisateurs, les developpeurs et les hébergeurs de site web de se protéger et de prévenir ce type d'attaque.

2 Principe de fonctionnement

2.1 Définition

La balise *iFRAME* est une balise *HTML*. Le nom *iFRAME* est utilisé pour désigner une `inline frame`. Cette balise est utilisée afin d'insérer dans une page *HTML* un autre document *HTML*.
Il est important de souligner la différence qui existe entre les balises *FRAME* et *iFRAME* :

- la balise *FRAME* est utilisée afin de diviser une page *HTML* en différentes pages organisées de manière logique. Ces pages sont toutes stockées sur le même serveur ;
- la balise *iFRAME* est, quant à elle, utilisée afin d'afficher au sein d'une même page des informations stockées sur des serveurs différents. Elle est, par exemple, souvent utilisée afin d'insérer des bandeaux publicitaires hébergés sur des serveurs dédiés.

2.2 Le code *HTML*

Voici, ci-dessous, l'exemple d'une page affichant un document *HTML* hébergé sur un autre serveur.

```
<html>
  <body>
Le site ci-dessous est une iFRAME vers le site www.certa.ssi.gouv.fr

        <iframe src="http://www.certa.ssi.gouv.fr/site/index.html" height="800" width="600"
            frameborder="0" scrolling="no">
        Texte fourni pour les navigateurs ne pouvant pas afficher une iFRAME
        </iframe>

  </body>
</html>
```

Il est possible de personnaliser la balise *iFRAME* avec les arguments suivants :

- `src` permet de définir la source du document à afficher à l'intérieur de l'*iFRAME* ;
- `height` et `width` definissent la taille de l'*iFRAME* ;
- `frameborder` permet de controler la taille des bordures de l'*iFRAME* ;
- `scrolling` paramètre la présence ou non d'une barre de défilement.

L'ensemble des spécifications de la balise *iFRAME* est disponible sur le site du `W3C` (cf. la section « Documentation »).

Lors de la visite de la page ci-dessus, l'internaute se connecte au serveur hébergeant la page. Comme la page en question contient une *iFRAME* intégrant le contenu de la page d'accueil du site http://www.certa.ssi.gouv.fr, le navigateur est dans l'obligation d'effectuer une deuxième connexion vers le site http://www.certa.ssi.gouv.fr afin d'afficher le contenu de la page http://www.certa.ssi.gouv.fr/site/index.html.

Cette deuxième connexion se fait de manière transparente pour l'utilisateur. Le navigateur affiche le contenu des deux pages téléchargées sur deux serveurs distincts sans que cela ne soit perceptible pour l'internaute.

3 Les risques liés à cette balise

La connexion de l'utilisateur au serveur hébergeant le contenu de l'*iFRAME* s'effectuant à son insu, il est facile pour un individu malveillant d'exploiter cette propriété afin de compromettre sa victime. L'objectif de l'utilisation de la balise *iFRAME* par une personne malintentionnée est bien souvent la propagation de codes malveillants.

Le mode opératoire est souvent le même. Le première étape est la compromission d'un site légitime. Une fois que l'attaquant a obtenu un accès au site, il en profite pour insérer dans les pages légitimes des *iFRAME* et les rendre invisibles. Pour cela, soit il en réduit la taille au minimum, soit il en bloque l'affichage. Le fait de bloquer l'affichage n'empêche en rien la connexion du visiteur vers le serveur contenant le contenu de l'*iFRAME*. Pour rendre l'*iFRAME* invisible aux yeux de l'internaute, il faut intégrer le paramètre suivant à la balise

```
style='display:none'
```

Le visiteur, se rendant sur la page d'un site a priori de « confiance », établit alors, à son insu, une connexion vers un site et télécharge un code malveillant. Ce code, pour s'exécuter, exploite des vulnérabilités du navigateur et s'installe sur la machine de la victime.

Les risques liés aux *iFRAME*s concernent les développeurs de sites Internet, les hébergeurs ainsi que les utilisateurs finaux.

Les développeurs sont la première barrière face à ce type d'attaque. L'injection de balise *iFRAME* dans une page web légitime s'effectue généralement par le biais d'une faiblesse du site Internet. La compromission d'un site peut nuire à l'image de son concepteur et de l'entité, entreprise ou administration, représentée par ce site.

Les hébergeurs, ayant un statut d'intermédiaire entre la conception du site et son utilisation finale, sont également concernés. Ils peuvent par leur vigilance, contrôle des journaux et mesure de filtrage, limiter ou même empêcher la compromission des sites et par conséquent des internautes visitant ces derniers.

Enfin les utilisateurs, naviguant sur l'Internet, peuvent être redirigés malgré eux vers des pages au contenu malveillant et ainsi compromettre leur système d'information. Ce risque existe également lors de réception de courriels si ces derniers sont envoyés et surtout lus au format *HTML*.

4 Les moyens de protection

La balise *iFRAME* est tout à fait légitime mais c'est l'utilisation qui en est faite qui la rend potentiellement dangereuse. Il est donc important de mettre en place certaines protections afin de limiter les risques et impacts des détournements de fonctionnalité qui peuvent en être fait. Les recommandations suivantes vont se faire sur trois niveaux afin de couvrir l'ensemble des acteurs concernés : l'utilisateur final, l'hébergeur, l'exploitant du site et le concepteur.

4.1 Les recommandations aux utilisateurs

Les moyens de protection décrits ci-dessous sont de manière générale des recommandations applicables pour toute navigation sur l'Internet :

- utiliser un compte utilisateur aux droits limités en particulier pour naviguer sur l'Internet ;
- maintenir l'ensemble des logiciels du système à jour (système d'exploitation, antivirus, navigateur, ...) ;
- désactiver par défaut l'interprétation de langage dynamique dans le navigateur (*JavaScript*, *Flash*, ...) ;
- filtrer via un serveur mandataire (local ou mutualisé) l'affichage des balises *iFRAME* ;
- lire les courriels au format texte.

4.2 Les recommandations aux hébergeurs

L'hébergement, surtout s'il est mutualisé (lire la note d'information CERTA-2005-INF-005 sur ce sujet) , est un point qui nécessite une attention particulière. Les recommandations sont les suivantes :

- maintenir à jour l'ensemble des logiciels du serveur ;
- cloisonner les données relatives aux différents sites lorsque l'hébergement est mutualisé. Cela permettra d'éviter une compromission en cascade de l'ensemble des sites ;
- analyser le contenu des pages et proscrire les balises *iFRAME* si ces dernières ne sont pas nécessaires au site ;
- contrôler l'intégrité des pages statiques afin de detecter toute modification illégitime du contenu.

4.3 Les recommandations aux exploitants du site web

Il est conseillé aux personnes en charge de la gestion du site Internet et de son contenu d'appliquer les recommandations suivantes :

- inspection régulière des journaux d'événements ;
- utlisation de mots de passe forts, particulièrement s'il existe une interface d'administration (voir la note d'information CERTA-2005-INF-001 sur les mots de passe) ;
- fermer les services inutiles (ftp, smtp, ...).

4.4 Les recommandations aux concepteurs/développeurs

La sécurité d'un site est en grande partie liée à son mode de conception et elle doit y être intégrée dès le départ. Afin de limiter les risques de compromission via une faiblesse de conception, il est recommandé de :

- contrôler les variables passées en paramètre lors de l'utilisation de langage de programmation comme PHP ou ASP, par exemple ;
- contrôler le format des variables si le site possède du contenu dynamique (forum, blog, ...) ;
- éviter l'utilisation de langage de programmation dynamique (*JavaScript*, *Flash*, ...) si cela n'est pas indispensable.

Le CERTA recommande également la lecture de sa note d'information CERTA-2007-INF-002 sur les bons usages de PHP.

5 Conclusion

La balise *iFRAME* peut permettre à une personne malintentionnée de forcer la connexion de l'utilisateur vers un site malveillant. Cette connexion peut permettre la compromission de la machine du visiteur soit par le téléchargement d'un code malveillant, soit par l'interprétation de code dynamique exploitant des vulnérabilités du navigateur. De plus, il est récurrent de constater l'imbrication d'*iFRAME* ce qui complique l'identification de la (ou des) machine(s) malveillante(s). Il est courant de constater qu'une *iFRAME* contient une ou plusieurs autres *iFRAME*. Cette cascade d'*iFRAME* pourrait permettre de mieux dissimuler les codes malveillants et faciliter l'ajout ou la suppression de vulnérabilités à exploiter.

Afin de limiter les risques liés à cette balise, il est important que tous les acteurs de l'Internet (des concepteurs aux utilisateurs finaux en passant par les hébergeurs) soient conscients de l'usage qui est faite de cette balise et des risques liés à son utilisation à des fins malveillantes.

6 Documentation

- Page de définition de la balise *iFRAME* sur le site de W3C :
  http://www.w3c.org/TR/html401/present/frames.html#edef-IFRAME
- Note d'information CERTA-2007-INF-002 du 20 mars 2007 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2007-INF-002
- Note d'information CERTA-2005-INF-001 du 12 avril 2007 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-001
- Note d'information CERTA-2005-INF-005 du 19 décembre 2005 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-005
- Bulletin d'actualité CERTA-2007-ACT-025 du 22 juin 2007 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2007-ACT-025

Gestion détaillée du document

17 juillet 2008 version initiale.