

Affaire suivie par :  
CERTA

## BULLETIN D'ACTUALITÉ

### Objet : Bulletin d'actualité 2012-10

---

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-2012-ACT-010>

---

### Gestion du document

Référence	CERTA-2012-ACT-010
Titre	Bulletin d'actualité 2012-10
Date de la première version	09 mars 2012
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 Prolongation des serveurs de remplacement « DNSChanger »

Dans l'article « Virus DNSChanger » du bulletin d'actualité CERTA-2012-ACT-008, le CERTA prévenait de la coupure des serveurs de remplacement mis en place par l'*Internet Storm Center* (ISC) le 8 mars 2012. Ceux-ci permettaient aux ordinateurs compromis par ces virus de conserver un accès aux services de l'Internet.

Une demande de l'ISC auprès de la justice américaine pour prolonger ce délai jusqu'au 9 juillet 2012 a été validée le 5 mars. Néanmoins, les opérations de détection et de correction préconisées dans l'article du bulletin d'actualité doivent être entreprises dès à présent.

### Documentation

- Bulletin d'actualité du CERTA CERTA-2012-ACT-008 :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2012-ACT-008/index.html>
- Message de l'ISC concernant le report de la coupure des serveurs DNS :  
<http://isc.sans.edu/diary.html?storyid=12652>

## 2 Compromission du site Web GitHub

*GitHub* est un site Web proposant l'hébergement de projets et la gestion de leur développement avec le système *Git*. Le 1er mars 2012, un utilisateur de ce service exposait une vulnérabilité présente dans tous les sites

qui reposent sur la technologie *Ruby on Rails* et qui utilisent une fonctionnalité spécifique de ce *framework* (ou « cadriciel ») sans respecter certaines préconisations de sécurité. Quelques jours plus tard, il s'octroyait les droits d'écriture dans la branche de développement de *Ruby on Rails*. Une analyse de cet incident, de la part des administrateur de *GitHub*, n'a pas mis en évidence d'acte véritablement malveillant, comme l'insertion d'un maliciel dans du code source des projets hébergés.

Toutefois, plusieurs enseignements sont à retenir :

- d'une part, il est nécessaire, lorsqu'un développement utilise du code obtenu sur des plates-formes communautaires, d'avoir la plus grande vigilance lors de l'import de ce code dans ce projet. En effet, la plate-forme hébergeant ce code n'est que très rarement contrôlée par son auteur ;
- d'autre part, un guide de développement *Ruby on Rails* (en anglais uniquement), se focalisant sur les aspects SSI, a été publié. Le CERTA encourage vivement les développeurs et administrateurs de sites Web sur *Ruby on Rails* de vérifier que les directives de ce guide sont bien suivies.

## Documentation

- Guide de développement *Ruby On Rails* :  
<http://guides.rubyonrails.org/security.html>
- Discussion initiale sur la présence de la vulnérabilité :  
<https://github.com/rails/rails/issues/5228>

## 3 Campagne de messages inhabituels

Le CERTA est informé d'une recrudescence des campagnes de messages électroniques non sollicités sous forme d'offres de recrutement. Ces messages, qui circulent aussi bien en français qu'en anglais, invitent le destinataire à déposer sa candidature pour des postes aux descriptions vagues, mais avec un salaire précis. Le champ *expéditeur* de ces messages est la plupart du temps falsifié, et différent de l'adresse à laquelle il faut renvoyer son CV.

Ces messages ne contiennent pas de pièce jointe malveillante et leur contenu leur permet souvent de traverser les filtres anti-spam. Il s'agit cependant d'ingénierie sociale ; destinée à collationner des informations, au mieux dans un but commercial, au pire pour réaliser « l'environnement » de personnels dans le cadre d'une opération plus vaste.

Contre l'ingénierie sociale, le CERTA recommande la sensibilisation régulière des utilisateurs.

## 4 Rappel des avis émis

Dans la période du 02 au 08 mars 2012, le CERTA a émis les publications suivantes :

- CERTA-2012-AVI-110 : Vulnérabilités dans Dotclear
- CERTA-2012-AVI-111 : Vulnérabilité dans Novell GroupWise
- CERTA-2012-AVI-112 : Vulnérabilité dans StoneGate
- CERTA-2012-AVI-113 : Vulnérabilité dans Ruby on Rails
- CERTA-2012-AVI-114 : Vulnérabilités dans Google Chrome
- CERTA-2012-AVI-116 : Vulnérabilité dans phpCAS
- CERTA-2012-AVI-117 : Vulnérabilité dans Novell ZENworks
- CERTA-2012-AVI-118 : Vulnérabilités dans MantisBT
- CERTA-2012-AVI-119 : Vulnérabilités dans Symantec Entreprise Vault
- CERTA-2012-AVI-120 : Vulnérabilités dans IBM Tivoli
- CERTA-2012-AVI-121 : Vulnérabilités dans IBM DB2
- CERTA-2012-AVI-122 : Vulnérabilités IBM Maximo
- CERTA-2012-AVI-123 : Vulnérabilités dans TrueType
- CERTA-2012-AVI-124 : Vulnérabilité dans RSA SecureID
- CERTA-2012-AVI-125 : Vulnérabilités dans ImageMagick
- CERTA-2012-INF-002 : Les défigurations de sites Web

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

- CERTA-2011-AVI-013-001 : Vulnérabilité dans sudo (ajout du bulletin de sécurité Gentoo)
- CERTA-2011-AVI-465-001 : Vulnérabilité dans stunnel (ajout du bulletin de sécurité Gentoo)
- CERTA-2012-AVI-028-002 : Vulnérabilité dans OpenSSL (ajout du bulletin de sécurité Gentoo)
- CERTA-2012-AVI-091-001 : Vulnérabilité dans libvorbis (ajout du bulletin de sécurité OpenSuse)
- CERTA-2012-AVI-094-002 : Vulnérabilité dans libxml2 (ajout du bulletin de sécurité Gentoo)
- CERTA-2012-AVI-115-001 : Vulnérabilités dans Adobe Flash Player (ajout du bulletin de sécurité RedHat)

## **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](http://www.ssi.gouv.fr/site_rubrique62.html)

## **Gestion détaillée du document**

**09 mars 2012** version initiale.