Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 03 février 2012
N° CERTA-2012-ACT-005

**Affaire suivie par :**
CERTA

# BULLETIN D'ACTUALITÉ

**Objet : Bulletin d'actualité 2012-05**



## Gestion du document

| | |
|---|---|
| Référence | CERTA-2012-ACT-005 |
| Titre | Bulletin d'actualité 2012-05 |
| Date de la première version | 03 février 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 Incident de la semaine

### 1.1 Infection par une archive Java

Le CERTA a été amené à traiter un incident sur un poste de travail sur lequel une archive Java a été téléchargée. L'extension des noms des fichiers d'archives Java est généralement JAR.

Les machines virtuelles Java, ou JVM, constituent une cible pour les codes malveillants. En effet, plusieurs versions de JVM peuvent cohabiter sur un même système. La mauvaise « bonne raison » de cette situation est un défaut de compatibilité ascendante à laquelle s'ajoute l'adhérence d'applications à telle ou telle version de la JVM. Une conséquence est que l'installation d'une version récente de JVM ne supprime pas une instance plus ancienne, laquelle peut être vulnérable. Réciproquement, une version vulnérable de JVM peut être installée sur un ordinateur, jusque là à jour, sans que l'utilisateur s'en rende compte parce que cette installation est noyée dans celle d'un autre produit, une suite bureautique, par exemple.

Cette situation côté client est aggravée par le trop rare recours des développeurs à la signature de leur code Java. Ce faisant les utilisateurs ne posent pas de restrictions sur les codes Java autorisés à s'exécuter sur leur poste. Les auteurs d'archives malveillantes ont donc leurs tentatives de pénétration facilitées.

**Recommandations**

Face à cette menace, il est recommandé, dans la mesure du possible et dans le respect de la politique de sécurité du SI :

- de vérifier que seules les versions indispensables des JVM sont présentes sur les ordinateurs ;
- de filtrer ou de bloquer le téléchargement d'archives Java ;
- de limiter l'exécution des programmes Java aux codes signés ;
- de signer les programmes légitimes développés en Java, de façon à pouvoir mettre en pratique la recommandation précédente ;
- de surveiller les flux entrant et sortant du SI à la recherche d'anomalies.

# 2 Alerte sur Cisco IronPort

## Les problèmes

Le CERTA a émis une alerte sur une vulnérabilité de certains boîtiers (*appliances*) Cisco IronPort.

Ces boîtiers embarquent un logiciel dérivé de BSD. La vulnérabilité sur le logiciel serveur Telnet de FreeBSD, corrigée par ce projet en décembre 2011, s'est répercutée sur des produits Cisco (et peut-être d'autres éditeurs). Elle est publique, ce qui en facilite l'exploitation.

Par ailleurs, par leurs fonctions, ces produits Cisco sont généralement placés en périphérie des SI. Cela a au moins deux conséquences. D'une part, ils sont exposés aux attaques provenant de l'extérieur du SI. D'autre part, si la vulnérabilité est exploitée avec succès, l'attaquant dispose d'un outil à son profit dont deux scénarios d'utilisation sont décrits ci-dessous.

Les boîtiers de filtrage de courriels analysent tous les messages électroniques entrant dans le SI. À supposer que l'attaquant installe un logiciel qui copie et renvoie tous les courriels vers un serveur sous son contrôle, il dispose d'un moyen formidable d'intelligence économique.

Les boîtiers qui filtrent les flux Web peuvent, de la même manière, être détournés et laisser les postes internes naviguer et recevoir les contenus de sites qui vont infecter ces postes.

Par ailleurs, et indépendamment de cette vulnérabilité, le protocole Telnet doit être délaissé au profit de protocoles sécurisés comme SSH. Dans son utilisation traditionnelle, Telnet véhicule en clair les informations de connexion, les rendant vulnérables à l'écoute. Le protocole SSH permet de sécuriser les connexions, mais encore faut-il que les paramètres d'utilisation présentent les qualités requises :

- la clef du serveur doit être de longueur suffisante ;
- le client doit utiliser une authentification adaptée. Le minimum est un mot de passe robuste. L'utilisation d'un certificat client est préférable, mais plus lourde à gérer.

## Recommandations

Si le CERTA recommande habituellement de procéder aux mises à jour dès que le correctif de sécurité est disponible, dans le cas présent, il recommande également :

- de désactiver le serveur Telnet et d'utiliser le protocole SSH avec des paramètres de qualité ;
- de limiter les adresses qui peuvent accéder à l'interface d'administration, dans une optique de défense en profondeur ;
- de multiplier les obstacles contre les attaques, de manière à ce que la compromission de boîtiers IronPort diminue le moins possible la protection des éléments sensibles du SI ;
- de surveiller les flux entrants et sortants du SI, à la recherche d'anomalies (protocole, destination, horaire, volume, motif d'URL...).

## Documentation

- Alerte du CERTA CERTA-2012-ALE-001 du 01 février 2012 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2012-ALE-001/index.html
- Avis du CERTA CERTA-2011-AVI-718 du 26 décembre 2011 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2011-AVI-718/index.html
- Note d'information du CERTA « Les mots de passe » :
  http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-001/index.html

– Mémento « La défense en profondeur appliquée aux systèmes d'information » :
http://www.ssi.gouv.fr/fr/bonnes-pratiques/outils-methodologiques/la-defense-en-profondeur-appliquee-aux-systemes-d-information.html
– Guide « Mécanismes cryptographiques : Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques » :
http://www.ssi.gouv.fr/IMG/pdf/RGS_B_1.pdf

# 3 Rappel des avis émis

Dans la période du 27 janvier 2012 au 02 février 2012, le CERTA a émis les publications suivantes :

– CERTA-2012-ALE-001 : Vulnérabilité dans Cisco IronPort
– CERTA-2012-AVI-034 : Vulnérabilité dans le noyau linux
– CERTA-2012-AVI-035 : Vulnérabilité dans Cisco IP Video Phone E20
– CERTA-2012-AVI-036 : Multiples vulnérabilités dans Postfix Admin
– CERTA-2012-AVI-037 : Vulnérabilité dans IBM solidDB
– CERTA-2012-AVI-038 : Vulnérabilité dans Samba
– CERTA-2012-AVI-039 : Vulnérabilités dans FFmpeg
– CERTA-2012-AVI-040 : Vulnérabilités dans SAP NetWeaver
– CERTA-2012-AVI-041 : Vulnérabilités dans IBM DB2 Accessories Suite
– CERTA-2012-AVI-042 : Vulnérabilité dans JBoss
– CERTA-2012-AVI-043 : Vulnérabilité dans IBM Web Experience Factory
– CERTA-2012-AVI-044 : Vulnérabilité dans RSA enVision
– CERTA-2012-AVI-045 : Vulnérabilité dans des produits Oracle
– CERTA-2012-AVI-046 : Vulnérabilités dans VMware ESX et ESXi
– CERTA-2012-AVI-047 : Multiples vulnérabilités dans les produits Mozilla
– CERTA-2012-AVI-048 : Vulnérabilité dans Ubuntu Software Properties
– CERTA-2012-AVI-049 : Vulnérabilité dans Ubuntu AccountsService
– CERTA-2012-AVI-050 : Vulnérabilités dans Apache
– CERTA-2012-AVI-051 : Vulnérabilité dans HP Network Automation
– CERTA-2012-INF-001 : Dénis de service - Prévention et réaction

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

– CERTA-2011-AVI-381-001 : Multiples vulnérabilités dans Bind (ajout du belletin de sécurité HP)
– CERTA-2011-AVI-580-002 : Vulnérabilités dans Java (ajout du bulletin de sécurité HP)
– CERTA-2011-AVI-645-001 : Vulnérabilité dans ISC BIND (ajout du bulletin de sécurité HP)
– CERTA-2012-AVI-006-001 : Multiples vulnérabilités dans OpenSSL (ajout du bulletin de sécurité HP)
– CERTA-2012-AVI-028-001 : Vulnérabilité dans OpenSSL (ajout du bulletin de sécurité Debian)

# 4 Actions suggérées

## 4.1 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.

### 4.2 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.

### 4.3 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.

### 4.4 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.

### 4.5 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.

### 4.6 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.

### 4.7 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

**03 février 2012** version initiale.