Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERT-FR

Paris, le 11 mai 2015
N° CERTFR-2015-ACT-019

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2015-ACT-019

1 - Fin de support Java 7

Depuis avril 2015, Oracle ne délivre plus de mises à jour et de correctifs de sécurité gratuits pour Java SE version 7 [1]. Oracle a démarré en janvier 2015 un processus de mise à jour automatique vers Java 8 [2] pour Windows 32-bit et OS X. Toutefois, de nombreuses installations de Java version 7 sont encore présentes sur les systèmes informatiques, notamment pour les autres systèmes d'exploitation qui nécessitent une mise à jour manuelle.

Pour faciliter la migration des applications existantes vers Java 8, Oracle a mis en ligne sur son site un guide d'adoption de Java 8 [3].

Le CERT-FR incite donc les administrateurs et les développeurs Java version 7 qui ne l'auraient pas déjà fait à migrer au plus vite vers une version supportée de Java (version 8). D'une manière générale, le CERT-FR recommande d'utiliser systématiquement la dernière version stable des produits et de veiller à la bonne mise à jour des correctifs de sécurité.

Documentation

1 Java SE 7 End of Public Updates Notice :
https://www.java.com/en/download/faq/java_7.xml
2 Java 7 Auto-Update to Java 8 :
http://www.oracle.com/technetwork/java/javase/downloads/autoupdatejre7tojre8-2389085.html
3 JDK 8 Adoption Guide :
http://www.oracle.com/technetwork/java/javase/jdk8-adoption-guide-2157601.html

2 - Résultats publics de cartographie Internet

Le CERT-FR constate des publications de plus en plus fréquentes de cartographies de serveurs accessibles depuis Internet. Ces cartographies, issues de balayages de port, sont réalisées à l'aide d'outils publics et des moyens limités.

Certains de ces résultats ont mis en évidence des vulnérabilités sur de nombreux systèmes d'information. Par exemple des listes d'adresses IP ont été publiées récemment concernant la présence des services suivants :

- modbus, utilisés principalement par des systèmes industriels [1] ;
- mongoDB, implémentant un serveur de base de données [2] ;
- memcached, utilisés principalement pour stocker des informations utilisées par un site Web [3] ;
- VNC ou RDP [4];
- etc.

Des outils en ligne réalisent également ce type de balayage de port de manière régulière et fournissent à leurs clients les résultats [5]. Dans la majorité des cas, un défaut de configuration est à l'origine de la vulnérabilité (filtrage trop permissif, absence d'authentification, etc.).

De plus, la multiplication des "objets connectés" (téléviseur, appareils électroménagers, etc.) reliés au réseau Internet augmente le nombre de systèmes potentiellement exposés sans que les utilisateurs soient préalablement avertis.

Le CERT-FR recommande de vérifier et de restreindre les accès aux services uniquement depuis les systèmes idoines. À ce titre l'ANSSI a publié des recommandations sur la configuration des services d'administration de système d'information [6].

Documentation

1 http://pierre.droids-corp.org/blog/html/2015/02/24/scanning_internet_exposed_modbus_devices_for_fun___fun.html
2 http://www.nextinpact.com/news/93037-mongodb-bdd-librement-accessibles-dont-celle-dun-operateur-francais.htm
3 http://media.blackhat.com/bh-us-10/presentations/Slaviero/BlackHat-USA-2010-Slaviero-Lifting-the-Fog-slides.pdf
4 http://w00tsec.blogspot.com/2014/08/scan-internet-screenshot-all-things.html
5 http://shodanio.wordpress.com
6 http://www.ssi.gouv.fr/guide/securiser-ladministration-des-systemes-dinformation/

3 - Délégation de privilèges sous Linux

Sur un système Linux, il est courant de déléguer certains privilèges à des catégories d'utilisateurs en fonction de leur besoin. Par exemple, il est courant de donner la possibilité à des administrateurs réseau de lancer la commande `tcpdump` en `root` afin d'effectuer des diagnostics. Cette délégation est souvent effectuée au moyen de la commande `sudo`. Ainsi, il est fréquent de voir la ligne suivante dans le fichier `/etc/sudoers` :

```
NETWORK_ADM ALL=(root) /usr/sbin/tcpdump
```

Cette approche constitue une faille de sécurité : en effet, le programme `tcpdump` permet de lancer des commandes arbitraires avec l'option `-z` (notamment utilisée pour compresser des captures réseau). Rien n'empêche une personne malintentionnée d'utiliser le programme `/bin/sh` pour obtenir les privilèges `root` à partir de la commande `sudo tcpdump`.

Une approche alternative est d'utiliser les *capabilities*, ou capacités Linux. Elles permettent de diviser les privilèges `root` en sous-parties plus restreintes. Ainsi, la commande `tcpdump` n'a besoin que de la capacité `CAP_NET_RAW` pour écouter sur le réseau. Il est donc possible d'affecter cette capacité au programme `tcpdump`, qui pourra alors être exécuté sans les privilèges `root` : la vulnérabilité dans la configuration `sudo` qui permettait d'élever ses privilèges a donc été corrigée. Il reste cependant un dernier problème à résoudre : affecter la capacité au programme permet à tous les utilisateurs de lancer `tcpdump`. Il faut alors restreindre l'utilisation de cette capacité au groupe des administrateurs réseau. Une première approche consiste à retirer les permissions d'exécution à tous les utilisateurs, et à les affecter aux administrateurs via un groupe Unix standard. Une seconde consiste à ne pas restreindre les droits sur l'exécutable `tcpdump`, mais plutôt à limiter les capacités héritables par les utilisateurs.

Le module PAM `pam_cap` permet de gérer finement les capacités que chaque utilisateur peut obtenir. Le module `pam_cap.so` doit être activé pour les différents types de connexions (SSH, `login`, etc.), par l'ajout de la ligne suivante en début des fichiers adéquats situés sous `/etc/pam.d/` :

```
auth required pam_cap.so
```

Le fichier `/etc/security/capability.conf` doit être édité pour indiquer quelle est la capacité dont peut hériter une liste d'utilisateurs (il n'est malheureusement pas possible de définir un groupe). Il faut ensuite interdire l'héritage des *capabilities* pour tous les autres utilisateurs avec la directive `none *`.

```
cap_net_raw user1 user2 [...]
none *
```

Le binaire `tcpdump` doit enfin être marqué comme s'exécutant avec la capacité `cap_net_raw` :

```
1. setcap cap_net_raw=ei /usr/sbin/tcpdump
```

Le fonctionnement des capacités liées aux fichiers est similaire à celui des programmes `setuid`. Le module `pam_cap` permet simplement de placer une limite haute aux capacités qu'un utilisateur peut obtenir.

Lors de la mise à jour du paquet `tcpdump`, il est fort probable que les capacités du binaire soient modifiées. La dernière opération indiquée ci-dessus sera alors à réitérer.

4 - Rappel des avis émis

Dans la période du 04 au 09 mai 2015, le CERT-FR a émis les publications suivantes :

- CERTFR-2015-AVI-199 : Multiples vulnérabilités dans ClamAV
- CERTFR-2015-AVI-200 : Vulnérabilité dans Squid
- CERTFR-2015-AVI-201 : Vulnérabilité dans IBM DB2 Connect
- CERTFR-2015-AVI-202 : Multiples vulnérabilités dans les produits Citrix
- CERTFR-2015-AVI-203 : Vulnérabilité dans Citrix NetScaler
- CERTFR-2015-AVI-204 : Multiples vulnérabilités dans Apache Tomcat
- CERTFR-2015-AVI-205 : Vulnérabilité dans Cisco UCS Central Software
- CERTFR-2015-AVI-206 : Multiples vulnérabilités dans Apple Safari

Gestion détaillée du document

11 mai 2015 version initiale.