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 03 août 2015
N° CERTFR-2015-ACT-031

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2015-ACT-031

1 - Élévation locale de privilèges dans Mac OS X 10.10

En juillet 2015, une vulnérabilité concernant le système d'exploitation Max OS X Yosemite (10.10) a été rendue publique par le chercheur en sécurité Stefan Esser. Cette vulnérabilité permet une écriture arbitraire de fichier pouvant conduire à une élévation locale de privilèges.

Vulnérabilité

Apple a introduit, dans la version 10.10 de son système d'exploitation Mac OS X, une fonctionnalité permettant de journaliser les erreurs de l'éditeur de lien dynamique dans un fichier spécifique plutôt que sur la sortie `stderr` (comportement par défaut). Le cas échéant, le chemin du fichier de destination doit alors être spécifié par l'utilisateur dans la variable d'environnement `DYLD_PRINT_TO_FILE`.

La vulnérabilité se situe dans le fait qu'aucune vérification des permissions n'est effectuée lors de l'accès au fichier.

Ainsi, l'usage de cette variable lors de l'exécution d'un binaire de type *Set UID* permet d'écrire un fichier dont le propriétaire est celui dudit binaire.

En effet, un binaire de ce type peut être exécuté par un utilisateur non privilégié tout en conservant les permissions associées à son propriétaire d'origine. Dans le cas où le propriétaire d'origine est l'utilisateur *root*, l'usage de cette variable permet alors une écriture arbitraire à n'importe quel endroit du système de fichiers.

La commande suivante permet de vérifier si un système est vulnérable :

```
$ EDITOR=/usr/bin/true DYLD_PRINT_TO_FILE=/vulnerable crontab -e
```

Cette commande exécute `crontab` en mode édition en utilisant le binaire `/usr/bin/true`. Son seul effet, si le système est vulnérable, est de créer le fichier `/vulnerable` car indiqué dans la variable d'environnement incriminée.

La commande `ls -la /` permet de vérifier la présence ou non du fichier à la racine :

```
$ ls -la /
total 314
...
-rw-r--r-- 1 root wheel 0 Dec 21 2012 vulnerable
...
```

Étant donné qu'il s'agit d'une écriture arbitraire de fichier avec des privilèges de super-utilisateur, il est possible d'exploiter cette vulnérabilité pour écrire directement un code exécutable permettant une élévation de privilèges.

Systèmes vulnérables

La fonctionnalité incriminée ayant été introduite dans la version 10.10 de Mac OS X, les versions antérieures ne sont pas concernées. Néanmoins, toutes les versions mineures allant de 10.10 à 10.10.4 sont vulnérables.

Atténuation des risques

Apple n'a pour le moment pas annoncé de disponibilité pour un correctif. Néanmoins, Stefan Esser propose une extension du noyau permettant d'atténuer les risques d'exploitation de la vulnérabilité. Cette extension utilise un grappin logiciel pour détecter l'exécution de binaires de type *Set-UID* et, le cas échéant, renomme à la volée toute variable d'environnement commençant par `DYLD_` (en remplaçant `DYLD_` par `XYLD_`).

Le code source de cette extension du noyau est disponible. Une version compilée et un paquetage d'installation ont aussi été publiés pour les personnes ne souhaitant pas compiler l'extension. Pour information, voici les condensats MD5 de ces deux binaires tels que téléchargés :

- `SUIDGuard.kext.tar.bz2` (extension seule) : `2196d910e971c44e1906ace39e317c99`
- `SUIDGuardNG-Installer.pkg` (paquetage) : `45ac83ced182f63e3a97f065cf893d2f`

Une fois l'extension installée et le système redémarré, il est conseillé de vérifier que cette dernière est correctement chargée avec la commande suivante :

```
$ kextstat -l | grep "com.sektioneins.driver.SUIDGuardNG"
56 0 0xffffff7f80a3e000 0x3000 0x3000 com.sektioneins.driver.SUIDGuardNG
    (1) <7 4 3 2 1>
```

Il est bon de noter que cette extension journalise toutes les neutralisations des variables d'environnement `DYLD_*`. La commande suivante permet de consulter les entrées correspondantes dans les journaux d'évènements du système :

```
$ cat /var/log/system.log | grep "SUIDGuard"
Jul 16 04:04:24 localhost kernel[0]: SUIDGuard: found and neutralized
    DYLD_ environment variable for SUID/SGID root binary
```

Aussi, à défaut de correctif ou de mise en place de l'extension noyau, la vulnérabilité nécessitant un accès local pour être exploitée, le CERT-FR recommande une vigilance accrue quant aux accès physiques à un système vulnérable et notamment l'application de bonnes pratiques de sécurité comme le verrouillage systématique des sessions ouvertes.

Documentation

- OS X 10.10 DYLD_PRINT_TO_FILE Local Privilege Escalation Vulnerability :
  https://www.sektioneins.de/en/blog/15-07-07-dyld_print_to_file_lpe.html
- Extension de noyau SUIDGuard :
  https://github.com/sektioneins/SUIDGuard
- Alerte du CERT-FR :
  http://www.cert.ssi.gouv.fr/site/CERTFR-2015-ALE-009

2 - Vulnérabilités des outils de type "bac à sable"

Le mardi 28 Juillet, le CERT-FR a publié l'avis CERTFR-2015-AVI-319 [1] concernant une vulnérabilité découverte puis corrigée dans le logiciel de virtualisation QEMU. L'envoi de certaines commandes ATAPI permettait de provoquer un dépassement de tampon sur le tas induisant notamment une exécution de code arbitraire sur le système hôte. Ainsi, un programme s'exécutant dans une machine virtuelle pourrait exploiter la vulnérabilité pour exécuter du code sur la machine hôte au même niveau de privilège que l'application QEMU.

Les solutions de virtualisation ont déjà fait l'objet de vulnérabilités similaires, à l'instar de la vulnérabilité Venom, décrite dans le bulletin d'actualité CERTFR-2015-ACT-023 [2] et de la vulnérabilité CVE-2015-3209 décrite dans l'avis CERTFR-2015-AVI-252 [3].

La virtualisation est souvent utilisée dans les domaines de l'hébergement d'infrastructure en nuage et dans l'analyse de logiciels malveillants pour observer leur comportement dans un environnement censé être contrôlé. Le CERT-FR rappelle, à la lumière des multiples vulnérabilités découvertes, qu'un environnement virtuel n'est pas une promesse de sécurité et d'isolation. Ceci est particulièrement vrai pour les outils de type "bac à sable" qui embarquent ces technologies.

Il est conseillé d'avoir un regard critique sur l'utilisation de ces outils et technologies ainsi que sur les conséquences que pourrait avoir leur compromission. Le CERT-FR recommande donc d'appliquer les principes de défense en profondeur et de moindre privilège. Il est par exemple possible de durcir le système d'exploitation en

utilisant SELinux et son implémentation pour la virtualisation : sVirt [4]. Il est également possible de limiter les privilèges des processus QEMU grâce à l'utilisation de surcouche de gestion telle que libVirt [5]. Enfin, l'application des mises à jour est indispensable.

Documentation

1 http://www.cert.ssi.gouv.fr/site/CERTFR-2013-AVI-319/
2 http://www.cert.ssi.gouv.fr/site/CERTFR-2015-ACT-023/
3 http://www.cert.ssi.gouv.fr/site/CERTFR-2015-AVI-319/
4 http://selinuxproject.org/page/SVirt
5 https://libvirt.org/drvqemu.htmlsecurity

3 - Rappel des avis émis

Dans la période du 27 juillet au 01 août 2015, le CERT-FR a émis les publications suivantes :

- CERTFR-2015-ALE-010 : Multiples vulnérabilités dans Google Android
- CERTFR-2015-AVI-319 : Vulnérabilité dans Xen
- CERTFR-2015-AVI-320 : Vulnérabilité dans Citrix XenServer
- CERTFR-2015-AVI-321 : Multiples vulnérabilités dans le noyau Linux Ubuntu
- CERTFR-2015-AVI-322 : Vulnérabilité dans ISC Bind
- CERTFR-2015-AVI-323 : Vulnérabilité dans Cisco IOS XE
- CERTFR-2015-AVI-324 : Multiples vulnérabilités dans le noyau Linux Ubuntu

Gestion détaillée du document

03 août 2015 version initiale.

Conditions d'utilisation de ce document :	`http://cert.ssi.gouv.fr/cert-fr/apropos.html`
Dernière version de ce document :	`http://cert.ssi.gouv.fr/site/CERTFR-2015-ACT-031`