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 14 décembre 2015
N° CERTFR-2015-ACT-050

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2015-ACT-050

1 - Procédure de montage d'image disque non standard

Cet article s'inscrit dans la continuité de ce qui a été publié dans le bulletin d'actualité CERTFR-2015-ACT-038, sur la copie de disque dur dans le cadre du traitement d'un incident de sécurité informatique. Les images acquises proviennent parfois d'environnements particuliers qui vont complexifier les méthodes pour lire les images des copies de disques, première étape dans l'analyse exhaustive d'un système.

Reconstruction d'un RAID

Lorsque du RAID logiciel est utilisé, il est conseillé dans tous les cas de récupérer les fichiers de configuration du RAID dans */etc/mdadm/mdadm.conf*, */etc/default/mdadm* et */etc/mdadm.conf*. Si l'analyste dispose d'une copie du bloc disque (*/dev/md**) il n'y a pas de reconstruction nécessaire, et la copie est utilisable avec les outils classiques :

- mount
- sleuthkit
- FTK Imager
- X-Ways
- Encase

En revanche, si les disques ont été copiés de manière fractionnée, il faut procéder à une reconstruction qui peut être plus ou moins aisée en fonction des informations disponibles et du type de RAID utilisé. Les exemples de commandes ci-dessous permettent de reconstruire un RAID5 à partir des copies de chaque périphérique type SCSI disk (*/dev/sd**).

Chaque partition ou disque constituant le RAID doit être initialisé en indiquant au système l'offset de début de la partition (cet offset est obtenu grâce à fdisk, ou mmls de sleuthkit) :

```
losetup -o <OFFSET> /dev/loop1 disk.raw
```

La commande suivante permet de sauvegarder la configuration RAID de chaque partition ou disque :

```
mdadm -examine /dev/loop1 >> conf_mdadm_loop.txt
```

Afin d'assembler les images sur le périphérique de bloc /dev/md0, il convient d'exécuter la commande suivante :

```
mdadm -assemble /dev/md0 /dev/loop1 [/dev/loop2 ...]
```

Il suffit alors de monter ce dernier pour accéder aux données :

```
mount -o ro /dev/md0 /mnt/evidence
```

Montage d'un volume logique

Pour faciliter l'exploitation d'un volume logique, il convient de préserver à l'avance les fichiers */etc/lvm/lvm.conf*, */etc/fstab* et */etc/mtab* qui donnent la configuration des volumes logiques.

Il est nécessaire de créer un périphérique de type loop pour chaque volume identifié dans la copie de disque, puis d'activer les groupes et les volumes avant de monter ce dernier.

Chaque groupe de volume doit être initialisé en indiquant au système l'offset de début du groupe :

```
losetup -r -o <OFFSET> /dev/loop1 disk.raw
```

Un groupe de volume que l'on appellera VG1 apparaît alors dans */dev/mapper*.

Pour le rendre actif :

```
vgchange VG1 -a y
```

L'opération doit être renouvelée pour les volumes logiques :

```
lvchange /dev/VG1/<partition> -a y
```

La partition est alors lisible :

```
mount -o ro /dev/mapper/VG1/<partition> /mnt/evidence
```

Dans certains cas, les 8 périphériques loop accessibles par défaut sur Linux peuvent ne pas suffire. Il est possible d'en augmenter le nombre disponible via la variable max_loop du fichier */etc/modules* (Debian).

Montage d'une image chiffrée

Microsoft BitLocker

Il est possible en environnement Windows d'utiliser le programme *manage-bde.exe*, qui permet de déchiffrer un volume BitLocker à l'aide de la phrase secrète de recouvrement, du mot de passe ou de la clé de recouvrement :

```
manage-bde.exe -unlock E: -pw
```

En environnement Linux, il existe un programme libre et gratuit nommé dislocker qui permet d'ouvrir un volume grâce à la phrase secrète de recouvrement ou du fichier BEK.

```
dislocker -v -V disk.raw -p<PHRASE_SECRETE> /tmp/
mount -o loop,ro /tmp/dislocker-file /mnt/evidence
```

LUKS

L'utilisation de LUKS peut être couplée avec les volumes logiques, il convient dans ce cas de préparer les groupes de volumes et les volumes logiques comme décrit précédemment.

Avant de monter la partition, il est nécessaire de déchiffrer le volume à l'aide de la phrase secrète :

```
cryptsetup -readonly luksOpen /dev/loop1 <volume>
```

Gestion d'un disque virtualisé

Les disques de machines virtualisées se présentent sous la forme de fichiers dans des formats différents, et peuvent faire l'objet d'une conversion dans un format brut pour plus de facilité d'utilisation. Les fichiers *.vmdk* pour VMWare, *.vdi* pour VirtualBox, *.img* pour Qemu et *.vhd* pour Hyper-V peuvent être convertis avec l'utilitaire qemu-img, libre et gratuit :

```
qemu-img converter -O raw <disque source> <disque destination>
```

Dans le cas de VMWare, il arrive parfois que les disques soient stockés en plusieurs fichiers (split). Afin de faciliter les manipulations, il convient de les rassembler en un fichier unique (flat).

```
vmware-vdiskmanager -r disk1.vmdk -t0 disk.vmdk
```

Il est ensuite possible de convertir, si besoin, le fichier au format brut avec l'outil qemu-img cité plus haut.

Documentation

- http://www.cert.ssi.gouv.fr/site/CERTFR-2015-ACT-038/
- http://www.qemu.org
- http://www.hsc.fr/ressources/outils/dislocker/

2 - Mise à jour mensuelle de Microsoft

Le 8 décembre, lors de sa mise à jour mensuelle, Microsoft a publié douze bulletins de sécurité dont huit considérés comme critiques et quatre comme importants :

- MS15-124 (critique) qui concerne Internet Explorer ;
- MS15-125 (critique) qui concerne Edge ;
- MS15-126 (critique) qui concerne les moteurs JScript et VBScript ;
- MS15-127 (critique) qui concerne le service Windows DNS ;
- MS15-128 (critique) qui concerne le composant graphique de Windows ;
- MS15-129 (critique) qui concerne Silverlight ;
- MS15-130 (critique) qui concerne Uniscribe ;
- MS15-131 (critique) qui concerne Office ;
- MS15-132 (important) qui concerne Windows ;
- MS15-133 (important) qui concerne le service PGM de Windows ;
- MS15-134 (important) qui concerne Windows Media Center ;
- MS15-135 (important) qui concerne les pilotes en mode noyau de Windows.

Le CERT-FR recommande l'application de ces correctifs de sécurité dès que possible.

Navigateurs

Cette mise à jour corrige 30 vulnérabilités dans Internet Explorer (bulletin MS15-125) et 15 vulnérabilités dans Edge (bulletin MS15-126). La plupart d'entre elles sont des corruptions de mémoire susceptibles de permettre une exécution de code arbitraire à distance. Parmi les autres, certaines permettent de contourner des mécanismes de sécurité tels que la disposition aléatoire de l'espace d'adressage mémoire ou le filtre de protection contre les injections indirectes de code transdomaines.

Bureautique

Plusieurs vulnérabilités de type corruption de mémoire ont également été corrigées dans Microsoft Office. Ces vulnérabilités sont susceptibles de permettre une exécution de code à distance lors de l'ouverture d'un fichier spécialement conçu.

Windows

Par ailleurs, la vulnérabilité CVE-2015-6175, qui porte sur une élévation de privilèges dans les pilotes de noyau de Windows, a été corrigée dans le bulletin MS-15-135.

Le CERT-FR attire l'attention de ses lecteurs sur le fait que, d'après Microsoft, cette vulnérabilité était exploitée dans le cadre d'attaques.

Documentation

- http://www.cert.ssi.gouv.fr/site/CERTFR-2014-AVI-375/index.html
- http://www.cert.ssi.gouv.fr/site/CERTFR-2014-AVI-376/index.html
- http://www.cert.ssi.gouv.fr/site/CERTFR-2014-AVI-377/index.html
- http://www.cert.ssi.gouv.fr/site/CERTFR-2014-AVI-378/index.html

3 - Rappel des avis émis

Dans la période du 07 au 13 décembre 2015, le CERT-FR a émis les publications suivantes :

- CERTFR-2015-AVI-519 : Multiples vulnérabilités dans Google Android (Nexus)
- CERTFR-2015-AVI-520 : Multiples vulnérabilités dans Microsoft Internet Explorer
- CERTFR-2015-AVI-521 : Multiples vulnérabilités dans Microsoft Edge
- CERTFR-2015-AVI-522 : Multiples vulnérabilités dans Microsoft JScript et VBScript
- CERTFR-2015-AVI-523 : Vulnérabilité dans Microsoft DNS

– CERTFR-2015-AVI-524 : Multiples vulnérabilités dans le composant graphique de Microsoft Windows
– CERTFR-2015-AVI-525 : Multiples vulnérabilités dans Microsoft Silverlight
– CERTFR-2015-AVI-526 : Vulnérabilité dans Microsoft Uniscribe
– CERTFR-2015-AVI-527 : Multiples vulnérabilités dans Microsoft Office
– CERTFR-2015-AVI-528 : Vulnérabilité dans Microsoft Windows PGM
– CERTFR-2015-AVI-529 : Multiples vulnérabilités dans Microsoft Windows
– CERTFR-2015-AVI-530 : Multiples vulnérabilités dans Microsoft Windows Media Center
– CERTFR-2015-AVI-531 : Multiples vulnérabilités dans les pilotes en mode noyau de Microsoft Windows
– CERTFR-2015-AVI-532 : Multiples vulnérabilités dans Apple iOS
– CERTFR-2015-AVI-533 : Multiples vulnérabilités dans Apple Safari
– CERTFR-2015-AVI-534 : Multiples vulnérabilités dans Apple OS X
– CERTFR-2015-AVI-535 : Multiples vulnérabilités dans Google Chrome
– CERTFR-2015-AVI-536 : Multiples vulnérabilités dans Adobe Flash Player
– CERTFR-2015-AVI-537 : Multiples vulnérabilités dans Citrix Xenserver
– CERTFR-2015-AVI-538 : Vulnérabilité dans Cisco Prime Collaboration Assurance
– CERTFR-2015-AVI-539 : Vulnérabilité dans Cisco Unified Computing System

Durant la même période, les publications suivantes ont été mises à jour :
– CERTFR-2015-AVI-418 : Multiples vulnérabilités dans Google Nexus (version initiale.)

Gestion détaillée du document

14 décembre 2015 version initiale.