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 20 juin 2016
N° CERTFR-2016-ACT-025

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2016-ACT-025

1 - Sécurité des conteneurs LXC

LXC (*Linux Containers*) est un système d'isolation de ressources pouvant être utilisé pour faire de la virtualisation « légère » : le noyau de l'hôte est partagé avec tous les systèmes invités.

LXC repose sur plusieurs mécanismes d'isolation fournis par le noyau Linux (*namespaces*, `cgroups`, `seccomp`).

Détection de l'exécution dans un conteneur

De nombreuses informations permettent à un utilisateur de savoir si le système dans lequel il se trouve est dans un conteneur. Parmi celles-ci, la présence des informations `container=lxc` dans les variables d'environnement du processus PID 1 indique que le système est dans un conteneur. L'opération de lecture nécessite cependant les privilèges `root`.

```
tr '\000' '\012' < /proc/1/environ
container=lxc
container_ttys=/dev/pts/0 /dev/pts/1 /dev/pts/2 /dev/pts/3
```

Si `systemd` est utilisé comme gestionnaire de services, il est possible de détecter, en tant qu'utilisateur non-privilégié, s'il s'agit d'un système invité (en conteneur ou machine virtuelle) en utilisant la commande `systemd-detect-virt`. Cette commande utilise le mécanisme présenté précédemment et, s'il échoue car l'utilisateur ne dispose pas des privilèges adéquats, vérifie le contenu du fichier `/run/systemd/container`. Ce fichier, géré par `systemd`, est en lecture pour tous et contient le mot `lxc` si le système est dans un conteneur.

De manière similaire, les versions d'Ubuntu fournies avec le gestionnaire de services `upstart` disposent du script `running-in-container` qui permet de détecter si le système est dans un conteneur en tant qu'utilisateur non-privilégié.

Certains *templates* montent la console et les TTY dans le répertoire `/dev/lxc` (directive `lxc.devttydir` dans le fichier de configuration). Si ce répertoire est présent, il est probable que le système soit dans un conteneur LXC.

Enfin, LXC crée une hiérarchie `cgroups` portant le nom `lxc` qui peut être visible dans l'arborescence du système de fichiers virtuel `sysfs` dans le système invité.

Évasion de conteneur

L'évasion d'un conteneur est moins triviale que l'évasion d'un `chroot`, mais elle reste cependant réalisable dans certains cas.

Si une vulnérabilité est présente dans le noyau, ce dernier étant partagé entre le conteneur et le système hôte, un attaquant pourra l'exploiter pour obtenir les privilèges les plus élevés sur le système hôte et s'évader du conteneur.

La sécurisation contre l'évasion repose principalement sur la configuration du conteneur. La restriction d'accès aux ressources de l'hôte, que ce soit les appels système ou les *devices*, est capitale.

Par exemple, Sebastian Krahmer a montré que l'utilisation de l'appel système `open_by_handle_at` conjointe avec la *capability* `CAP_DAC_READ_SEARCH` permet à un attaquant de lire toute une partition sur l'hôte dont un répertoire est monté en *bind mount* dans le conteneur (cf. Documentation). En particulier, si ce répertoire est présent sur la partition `root`, l'attaquant pourra accéder au fichier de base de mots de passe `/etc/shadow`, et ainsi faciliter le rebond sur l'hôte.

De même, l'absence de restriction d'accès aux *devices* représentant les partitions des disques durs de l'hôte permet de s'échapper du système invité. Il suffit pour cela de monter la partition racine de l'hôte dans un répertoire du système invité, comme cela se fait pour l'évasion de `chroot`. Par défaut, la gestion de l'accès aux *devices* sous LXC fonctionne par liste blanche, c'est-à-dire que l'accès à toutes les ressources du système hôte est interdit, puis sont autorisées au cas par cas uniquement celles nécessaires au bon fonctionnement du système invité. Les *devices* représentant les partitions des disques durs de l'hôte ne sont pas autorisées dans la configuration par défaut.

Recommandations

Il est recommandé de considérer le compte `root` au sein des conteneurs privilégiés comme étant aussi important que le compte `root` du système hôte.

La sécurité d'un conteneur repose tout d'abord sur la mise à jour du système hôte (noyau et applications LXC).

Afin de limiter l'étendue d'une éventuelle évasion, un profil SeLinux, AppArmor ou autre LSM (*Linux Security Module*) peut être appliqué à chaque conteneur.

Enfin, un durcissement supplémentaire du noyau, au travers du patch `grsecurity` par exemple, permet de limiter la possibilité d'évasion par exploitation d'une vulnérabilité noyau. Il faut cependant noter que certaines fonctionnalités du patch sont incompatibles avec l'utilisation de conteneur ou des LSM.

La sécurité d'un conteneur privilégié repose aussi sur sa configuration. Celle créée par défaut par LXC permet d'avoir un niveau de sécurité minimum. Elle ne doit en aucun cas faire l'objet d'assouplissement. Le durcissement de cette configuration peut se faire – après analyse – par :

- l'ajout d'appels système dans la liste noire `seccomp` (liste des appels système interdits à l'intérieur du conteneur) ;
- l'ajout de *capabilities* dans la liste noire ;
- la suppression d'accès à certaines ressources grâce aux `cgroups`.

Les conteneurs non privilégiés reposent sur la fonctionnalité *user namespace* et sur son mécanisme d'*uid mapping*, ce dernier étant disponible à partir de la version 3.18 du noyau *vanilla* de Linux.
De nombreuses vulnérabilités sur l'implémentation de cette fonctionnalité ont été récemment publiées. Certaines distributions, telles que ArchLinux, l'ont ainsi donc désactivée.
À terme, les conteneurs non privilégiés permettraient de limiter l'étendue d'une compromission sur l'hôte aux seuls objets accessibles par l'utilisateur ayant lancé le conteneur. Cependant, en l'état actuel de l'implémentation des *user namespaces*, tous les conteneurs LXC doivent être considérés comme des conteneurs privilégiés.

Documentation

- Démonstration par Sebastian Krahmer de l'accès possible aux fichiers de l'hôte depuis un conteneur : http://stealth.openwall.net/xSports/shocker.c

2 - Mise à jour mensuelle de Microsoft

Le 14 juin, lors de sa mise à jour mensuelle, Microsoft a publié seize bulletins de sécurité, dont cinq considérés critiques et onze importants :

- MS16-063 (critique) concernant Internet Explorer ;
- MS16-068 (critique) concernant le navigateur Edge ;
- MS16-069 (critique) concernant JScript et VBScript ;
- MS16-070 (critique) concernant Microsoft Office ;
- MS16-071 (critique) concernant le serveur DNS Microsoft Windows ;
- MS16-072 (important) concernant la stratégie de groupe ;
- MS16-073 (important) concernant les pilotes en mode noyau Windows ;
- MS16-074 (important) concernant le composant graphique de Microsoft ;
- MS16-075 (important) concernant le serveur SMB Windows ;

– MS16-076 (important) concernant Netlogon ;
– MS16-077 (important) concernant WPAD ;
– MS16-078 (important) concernant le concentrateur de diagnostic Windows ;
– MS16-079 (important) concernant Microsoft Exchange Server ;
– MS16-080 (important) concernant PDF Microsoft Windows ;
– MS16-081 (important) concernant Active Directory ;
– MS16-082 (important) concernant Microsoft Windows Search.

Navigateurs

Cette mise à jour corrige dix vulnérabilités dont sept considérées critiques dans Internet Explorer. Ces dernières permettent une exécution de code à distance.
Deux d'entre elles (les vulnérabilités CVE-2016-0199 et CVE-2016-0200) sont causées par la manière dont Internet Explorer traite les objets en mémoire.
Les cinq autres proviennent de vulnérabilités d'altération de mémoire dans le moteur de script.
Parmi les trois vulnérabilités restantes, jugées importantes, les vulnérabilités CVE-2016-3211 et CVE-2016-3212 permettent une exécution de code à distance. Cette dernière provient d'un problème du filtre XSS dans Internet Explorer. La vulnérabilité CVE-2016-3213 peut déboucher sur une élévation de privilège lors de l'utilisation du protocole Web Proxy Auto Discovery (WPAD) dont l'implémentation est vulnérable et permet à un attaquant de répondre à une requête de nom NetBIOS.

Huit vulnérabilités ont été corrigées dans Microsoft Edge. Cinq d'entre elles peuvent déboucher sur une exécution de code à distance, dont la CVE-2016-3203 qui peut être exploitée si un utilisateur ouvre un fichier PDF piégé.
Les vulnérabilités CVE-2016-3201 et CVE-2016-3215 permettent d'obtenir des informations sensibles dans le contexte de l'utilisateur actuel en utilisant également un fichier PDF comme vecteur d'attaque.
La dernière vulnérabilité affectant Edge (CVE-2016-3198) était un contournement de la politique de sécurité qui pouvait arriver lorsque la stratégie de sécurité de contenu (CSP) ne parvenait pas à valider correctement certains contenus.
À noter que la vulnérabilité CVE-2016-3222 a été publiée, cependant aucune exploitation active n'a été constatée.

Bureautique

La suite Office de Microsoft a reçu quatre correctifs de sécurité. Trois d'entre elles pour de potentielles exécutions de code à distance. La CVE-2016-0225 est jugée critique, car le volet de visualisation peut être un vecteur d'attaque si l'utilisateur reçoit un courrier électronique piégé.
La vulnérabilité CVE-2016-3234 peut déboucher sur une divulgation d'information lors de l'ouverture d'un document conçu de manière malveillante.

Windows

Les vulnérabilités critiques CVE-2016-3205, CVE-2016-3206, CVE-2016-3207 touchent les moteurs de script Jscript et VBScript et permettent un exécution de code à distance. Elles sont aussi référencées dans le bulletin concernant Internet Explorer (MS16-063).

La dernière vulnérabilité jugée critique est notée CVE-2016-3227 et permet également une exécution de code à distance. Elle touche le serveur DNS de Windows et peut être exploitée par une requête malveillante profitant d'une condition d'utilisation après libération.

De multiples vulnérabilités dont l'exploitation permet une élévation de privilèges ont été corrigées dans la stratégie de groupe (CVE-2016-3223), dans Win32k (CVE-2016-3218, CVE-2016-3219 et CVE-2016-3221), dans Adobe Type Management Font Driver (ATMFD.dll, CVE-2016-3220), dans le serveur SMB (CVE-2016-3225), dans WPAD (CVE-2016-3213 et CVE-2016-3236) ainsi que dans le concentrateur de diagnostic Windows (CVE-2016-3231).
À noter que la vulnérabilité, CVE-2016-3236 a été révélée publiquement, mais n'a pas fait l'objet d'exploitation active.

Quatre vulnérabilités de divulgation d'informations ont reçu un correctif. La première (CVE-2016-3232) dans le composant virtuel PCI de Windows, car le fournisseur de service virtuel ne gère pas correctement la mémoire non initialisée. La deuxième (CVE-2016-3216) touche le composant graphique de Windows. Une exploitation réussie

permettrait à un attaquant de récupérer des informations facilitant le contournement de la disposition stochastique de l'espace mémoire (ASLR). Les deux dernières (CVE-2016-3201 et CVE-2016-3215) concernent Windows PDF et ont déjà été évoquées dans la section consacrée aux navigateurs.

Deux vulnérabilités importantes susceptibles de provoquer une exécution de code à distance ont été corrigées. La CVE-2016-3203 concerne aussi Windows PDF et est ainsi référencée dans le bulletin MS16-068 dédié à Edge. La vulnérabilité CVE-2016-3228 peut être exploitée par le biais d'une requête NetLogon spécialement conçue à destination d'un contrôleur de domaine.

La vulnérabilité CVE-2016-3230 concerne le composant Windows Search et la manière dont celui-ci traite les objets en mémoire, ce qui peut entraîner un déni de service. À noter que cette vulnérabilité a été aussi été publiée, mais là encore, aucune exploitation active n'a été constatée.

Les serveurs Microsoft Exchange ont reçu plusieurs correctifs. La vulnérabilité CVE-2016-0028 peut être exploitée en contournant le filtre du courrier électronique en profitant de la manière dont le serveur analyse les requêtes HTML. Cela permet à un attaquant d'identifier et de suivre un utilisateur en ligne. Trois autres vulnérabilités (CVE-2016-6013, CVE-2016-6014, CVE-2016-6015) peuvent conduire à une élévation de privilège dans les bibliothèques Oracle Outside suite à des débordements potentiels de la mémoire tampon.

Pour finir, une vulnérabilité de déni de service dans Active Directory a été comblée (CVE-2016-3226).

Recommandations

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

3 - Rappel des avis émis

Dans la période du 13 au 19 juin 2016, le CERT-FR a émis les publications suivantes :

- CERTFR-2016-ALE-004 : Vulnérabilité dans Adobe Flash Player
- CERTFR-2016-AVI-200 : Multiples vulnérabilités dans Keepass 2
- CERTFR-2016-AVI-201 : Vulnérabilité dans Adobe ColdFusion
- CERTFR-2016-AVI-202 : Vulnérabilité dans VMware vCenter Server
- CERTFR-2016-AVI-203 : Multiples vulnérabilités dans Microsoft Internet Explorer
- CERTFR-2016-AVI-204 : Multiples vulnérabilités dans Microsoft Edge
- CERTFR-2016-AVI-205 : Multiples vulnérabilités dans Microsoft Word
- CERTFR-2016-AVI-206 : Multiples vulnérabilités dans Microsoft Windows
- CERTFR-2016-AVI-207 : Multiples vulnérabilités dans Microsoft Exchange Server
- CERTFR-2016-AVI-208 : Vulnérabilité dans Microsoft Active Directory
- CERTFR-2016-AVI-209 : Multiples vulnérabilités dans les produits Cisco
- CERTFR-2016-AVI-210 : Multiples vulnérabilités dans Drupal Core
- CERTFR-2016-AVI-211 : Vulnérabilité dans Citrix iOS Receiver
- CERTFR-2016-AVI-212 : Vulnérabilité dans SCADA Schneider Electric Pelco Digital Sentry Video Management System
- CERTFR-2016-AVI-213 : Multiples vulnérabilités dans Adobe Flash Player
- CERTFR-2016-AVI-214 : Multiples vulnérabilités dans Google Chrome

Gestion détaillée du document

21 juin 2016 version initiale.