

Sécurité des systèmes d'information

Devoir 1 - Élévation de privilèges

Equipe : Chaimaa Zegoumou, Ayoub Nasr, Hamza Tamenaoul.

1 Analyse de faille

- **Service compromis :** Oracle Solaris 11.
- **Type de compromission :** Privilege escalation.
- **Explication de la vulnérabilité :**

Du à une erreur de conception dans xscreensaver, en tant qu'attaquant local, on peut créer des fichiers arbitraires sur le système en abusant de l'option -log. L'exploitation de cette faille peut avoir pour but la provocation d'un déni de service (DDoS) ou d'acquérir les privilèges root.

On se sert de la technique **LD_PRELOAD**. Cette dernière est une variable d'environnement qui permet de spécifier une bibliothèque chargée au démarrage d'un programme. Pour élever les privilèges à ceux de root, on crée en tant qu'utilisateur local non root le fichier getuid.c qui retourne suite à l'appel à getuid() la valeur 0 correspondant bien au uid du root. On compile ensuite ce fichier. Le coeur de la faille réside dans l'option log de xscreensaver : grâce à cette option, on crée un fichier dans le path - ce qui nous est normalement interdit en tant qu'utilisateur non root - /usr/lib/secure/64 avec les droits d'accès 666. Ce fichier nous servira plus tard comme librairie à précharger avant de lancer la commande 'su -' par LD_PRELOAD.

Ensuite, on recopie le contenu du fichier getuid.so dans le fichier de logs de xscreensaver. En redéfinissant LD_PRELOAD comme suit :

"LD_PRELOAD=/usr/lib/secure/64/getuid.so su -" , et on lance la commande "su -". On devient root.

2 Préconisations

Vu l'impact que cette vulnérabilité peut avoir sur le système, il est urgent de pouvoir prendre des mesures afin de limiter les dégats qu'elle peut avoir. Ces mesures peuvent prendre la forme de deux actions différentes :

- Vu que cette faille joue sur la possibilité de Xscreensaver de pouvoir changer les droits sur les fichiers. Ceci peut s'avérer un peu difficile, contre productif, et peut encore conduire à des dysfonctionnements au niveau de Xscreensaver.
- La solution qui reste la plus optimale, efficace, et facile par ailleurs est d'installer le patch d'urgence lancé par Oracle afin de régler le problème une fois pour toute. Oracle a en effet notifié tous les utilisateurs ayant un système qui peut être compromis de l'importance de la mise à jour, et un test de la faille a été aussi divulgué pour permettre de tester son système contre cette vulnérabilité.

Ainsi, parmi les bonnes pratiques qui doivent être prises en compte en général dans les systèmes d'informations et les infrastructures logicielles, les plus utiles dans ce cas sont :

- Toujours donner le minimum de droits nécessaires. Cette règle très connue est souvent mal appliquée vu la charge de travail qu'elle implique, cependant elle reste très efficace dans beaucoup de cas. Il faut aussi faire attention au fait que cette règle ne s'applique pas seulement aux usagers du système, mais aussi aux différents logiciels qui sont installés sur le système, et qui pour beaucoup ont des droits très importants.
- De plus, il faut aussi faire attention à que notre système soit toujours à jour. Souvent, les mises à jour apportent des patches à des failles de sécurité qui peuvent éviter de grands dangers. Cette règle devient d'autant plus importante à appliquer dans le cas des mises à jour de sécurité.
- Ne pas permettre aux utilisateur d'installer n'importe quel programme sur la machine, en l'occurrence dans notre cas les programmes telle que gcc ou bien encore Xscreensaver.

2.1 Point de vue entreprise de développement de logiciel

En étudiant l'origine de la faille, on se rend compte que cette faille est spécifique à la plateforme Oracle pour une raison simple : Le logiciel distribué par Oracle n'est pas issu de la codebase courante du programme, mais d'une version modifiée basée sur une ancienne codebase de 2002. Ce qui nous permet d'en déduire la règle suivante :

- Lorsqu'on utilise le code d'un logiciel libre pour développer une brique plus grosse comme dans ce cas, il faut toujours être à l'écoute des différentes failles de sécurité qui peuvent être déclarées dans le programme et de leurs corrections. Si ceci avait été fait dans ce cas, cette faille n'aurait pas eu lieu d'exister vu qu'elle a déjà été corrigée, il y a plus d'une dizaine d'années.

3 PSSI

Description de l'entreprise : Une entreprise qui, parmi ses activités, traite des données bancaires, dispose d'un serveur central dont les employés ont accès, qui abrite la plupart des données et logiciels de l'entreprise et tourne sous Solaris 11.4 d'Oracle.

Niveau de sensibilité : Très sensible vu qu'elle traite des données bancaires, et les logiciels installés sur ces serveurs peuvent interagir avec le réseau interbancaire.

Topologie des données : Les données sont stockées sur le serveur central en intégralité.

Niveau de criticité : Perte de confidentialité entraînant des pertes dommageables.

Actions préventives et curatives :

- Désinstaller les compilateurs potentiellement installés sur le système.
- Impliquer les employés et les sensibiliser quant à l'existence d'une telle faille dans le but d'éviter qu'un des employés ne donne accès à sa machine à une personne qui peut compromettre le système.
- Bloquer l'installation de programmes telle que gcc qui sont fondamentaux à l'exploitation de la faille.
- Créer des groupes d'utilisateurs et les assigner aux utilisateurs qui ne sont pas censés avoir des privilèges root comme groupe principal, puisque par défaut, tout utilisateur créé a le groupe 'staff' comme son groupe principal, qui a des droits root sur plusieurs répertoires et fichiers, ce qui a été justement l'une des raisons pour lesquelles la vulnérabilité existe.

4 Mise en évidence de la vulnérabilité

Afin de mettre en évidence l'exploitation de cette faille, on a mis en place une machine virtuelle dont la création est automatisée par le biais de Vagrant. On utilise comme image source celle de Solaris 11.4, et on y installe ensuite les outils nécessaires pour reproduire l'exploit (compilateur gcc, solaris-desktop qui contient xscreensaver, le logiciel compromis, ainsi que l'écosystème nécessaire pour son exécution).

Vu que l'attaque peut se faire en tant qu'utilisateur non root et que la connexion par ssh à cette machine nous connecte directement par un utilisateur aux privilèges root, on vous dicte alors les étapes suivantes pour reproduire facilement l'exploitation de cette faille. Une explication plus détaillée de l'exploit est en partie "1-explication de la vulnérabilité".

1. Créer un utilisateur par le biais de la commande :

```
sudo useradd -m testUser
```

2. Rajouter un mot de passe pour cet utilisateur.

```
sudo passwd testUser
```

3. Se connecter en tant que *testUser*

```
su testUser
```

4. Copier le contenu du fichier 'exploit.sh' dans l'archive fournie et créer un fichier 'exploit.sh' dans le dossier /export/home/testUser.

5. Permettre l'exécution de ce script par le biais de :

```
chmod +x exploit.sh
```

6. Lancer le script, après son exécution, on se retrouve en tant que root.

5 Références

- Marco Ivaldi, <https://techblog.mediaservice.net/2019/10/local-privilege-escalation-on-solaris-11>
- <https://nvd.nist.gov/vuln/detail/CVE-2019-3010>
- https://techblog.mediaservice.net/2019/10/local-privilege-escalation-on-solaris-11/?fbclid=IwAR37EyX6yKhj25qXPGFuV3c3JzHhARW5mx3Qm20d_LQcnDSnGZMx0tR_BGY
- <https://github.com/oracle/solaris-userland/blob/18c7129a50c0d736cbac04dcfbfa1502ea/components/desktop/xscreensaver/patches/0005-gtk-lock.patch#L3749-L3770>
- <https://src.fedoraproject.org/rpms/xscreensaver/blob/9a0bab5a19b03db9671fc5a207147f/xscreensaver.spec#L2178-2179>