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 31 janvier 2014
N° CERTFR-2014-ACT-005

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2014-ACT-005

1 - Comptes de service en environnement AD (première partie)

Cet article est le premier d'une série de 3 articles relatifs aux comptes de service. Seront abordées dans cette série les thématiques suivantes :

- contexte, problématique et maîtrise des comptes de service
- techniques d'identification des comptes de service
- technologies créées par Microsoft pour faciliter la gestion des comptes de service

Cet article détaille le contexte et la problématique liés à la maîtrise des comptes de service.

Description des comptes de service

Les comptes de service sont des comptes (locaux ou centralisés) utilisés par des traitements automatiques. Ils ont ainsi la particularité d'avoir généralement leur mot de passe stocké en dur dans le code des applications, dans un conteneur du système d'exploitation ou dans des fichiers de configuration.

Il faut noter qu'un compte de service peut également correspondre au compte d'une personne, ce qui est une déviance dans les pratiques d'administration. Dans ce cas, il est nécessaire de le considérer comme un compte de service.

Cet article se focalise sur la problématique de gestion de ces comptes en environnement Active Directory.

Problématique des comptes de service dans un contexte Active Directory

Exposition

Le fait que le mot de passe des comptes de service soit inscrit dans un fichier de configuration ou dans le registre d'un système Windows facilite sa récupération par une personne malveillante. Plusieurs moyens peuvent être utilisés par un attaquant pour cela : compromission du système sous-jacent, abus d'un problème de droits sur un fichier contenant le mot de passe, exploitation d'une vulnérabilité dans l'application qui l'utilise permettant d'accéder à un fichier de configuration, etc.

Droits

Il est tentant d'affecter des droits élevés aux comptes de service, afin de se prémunir contre des dysfonctionnements liés à des droits d'accès insuffisants.

Dans la pratique, il n'est pas rare que des comptes de service soient placés dans les groupes natifs d'administration de l'Active Directory (« Administrateurs du domaine », « Administrateurs de l'entreprise », « Administrateurs du schéma », « Administrateurs ») ou dans les groupes des opérateurs (« Opérateurs de compte », « Opérateurs de sauvegarde », « Opérateurs de serveur », « Opérateurs d'impression », « Duplicateurs », « Éditeurs de certificats », « Générateurs d'approbations de forêt entrante », etc.).

Si une personne malveillante parvient à compromettre le mot de passe d'un tel compte, elle obtient donc beaucoup de droits et privilèges au niveau du domaine.

Changement du mot de passe

Le mot de passe d'un compte de service étant potentiellement stocké à différents endroits du système d'information, il peut être compliqué de procéder à son changement. Il est donc tentant de supprimer l'expiration automatique du mot de passe généralement imposée par la politique en vigueur au niveau de l'Active Directory.

Si une personne malveillante vient à prendre connaissance d'un mot de passe n'expirant pas, elle est en mesure de le réutiliser sans restriction de durée.

Les conséquences sont aggravées si le compte de service correspond également à un utilisateur, car la personne malveillante aurait, de plus, accès aux ressources de celui-ci (messages électroniques, documents, etc.). Il en résulte également une perte de traçabilité, en temps normal et en cas de compromission, car l'activité de l'attaquant sera plus difficile à distinguer.

Maîtrise des comptes de service

Afin d'être en mesure de maîtriser l'utilisation des comptes de service (changement de mots de passe, traçabilité d'utilisation, etc.), il est nécessaire de documenter leur emploi.

Un document doit ainsi recenser tous les comptes de service et leur utilisation. Il doit contenir pour chaque compte de service identifié :

- les informations concernant le compte (SamAccountName, description, groupes AD d'appartenance, caractéristiques UserAccountControl, etc.)
- les applications (ou les systèmes) qui utilisent le compte ;
- la date de dernier changement du mot de passe associé au compte ;
- la procédure de changement du mot de passe du compte.

Par ailleurs, pour chaque compte de service appartenant aux groupes privilégiés, il convient :

- de définir et de justifier les privilèges strictement nécessaires en fonction des applications concernées, en lien avec les équipes projet ;
- d'appliquer les nouveaux privilèges si nécessaire.

Comme tout compte particulier du domaine, les comptes de service doivent respecter une nomenclature particulière (préfixe ou suffixe caractéristique), afin de pouvoir rapidement les identifier dans un groupe ou dans les journaux de sécurité.

Sauf cas particuliers, les comptes de service doivent être bloqués sur un relais Web afin d'empêcher leur utilisation pour la navigation sur Internet et réduire les possibilités d'exfiltration automatisée de données.

Le prochain article de cette série abordera les techniques d'identification de la majorité des comptes de service dans un environnement Active Directory.

2 - Incident et politique de journalisation

Les fichiers de journalisation peuvent être particulièrement utiles dans le traitement d'un incident. Le CERT-FR constate cependant fréquemment que la politique de journalisation deployée sur les serveurs et les postes client est inadaptée, réduisant ainsi considérablement la quantité de données exploitables pour appréhender les incidents.

Dans une affaire traitée récemment par le CERT-FR, des tentatives de connexions répétitives suspectes sur un compte administrateur ont été identifiées, entraînant un blocage de ce compte. Bien que journalisés sur un contrôleur de domaine, les événements liés aux connexions d'un utilisateur ne sont pas journalisés journalisés par défaut sur le poste de travail lui-même. L'origine de ces tentatives a donc été particulièrement difficile à déterminer. L'application d'une politique de journalisation appropriée a permis de récolter les données techniques utiles (connexions réussies et échouées). Il a ainsi pu être établi que les connexions suspectes étaient dues à un processus légitime mal configuré et non à une tentative de compromission.

Le niveau de journalisation par défaut d'un système dépend du type de système d'exploitation et de sa fonction (poste de travail, serveur). Il appartient donc aux administrateurs d'appliquer une politique de journalisation suffisamment fine permettant de détecter des évènements anormaux, les qualifier et, au besoin, de mener des investigations approfondies. La politique de journalisation doit notamment préciser les conditions de conservation des

journaux (période de rétention, sauvegarde, protection, etc.). Cette politique devra s'appliquer à tous les éléments du réseau (serveurs mandataires, pare-feu, etc).

L'ANSSI a publié un ensemble de recommandations de sécurité pour la mise en oeuvre d'un système de journalisation.

Documentation

- Recommandatations de sécurité pour la mise en oeuvre d'un système de journalisation : http://www.ssi.gouv.fr/fr/guides-et-bonnes-pratiques/recommandations-et-guides/securite-du-poste-de-travail-et-des-serveurs/recommandations-de-securite-pour-la-mise-en-oeuvre-d-un-systeme-de.html

3 - Option -fstack-protector-strong de GCC 4.9

La version de développement de GCC (4.9) propose une nouvelle fonctionnalité pour protéger les programmes des tentatives d'exploitation de vulnérabilités de type débordement de tampon sur la pile.

Pour rappel, l'exploitation de ce type de vulnérabilité repose sur la possibilité, en effectuant un débordement de tampon, de réécrire sur la pile l'adresse de retour de la fonction (saved EIP) pour détourner le flot d'exécution d'un programme.

Cette nouvelle fonctionnalité s'appelle `-fstack-protector-strong` et correspond à une amélioration de `-fstack-protector` et `-fstack-protector-all`. Avant de présenter le fonctionnement de cette nouvelle fonctionnalité, il est important de revenir, dans un premier temps, sur les options `-fstack-protector` et `-fstack-protector-all`.

Par défaut, GCC active entre autres l'option de sécurité `FORTIFY_SOURCE` qui permet de détecter certains débordements de tampon ou des corruptions mémoire, comme par exemple les vulnérabilités de mise en forme de chaînes (Format string). Cette fonctionnalité ne sera pas abordée et sera désactivée dans les exemples fournis par la suite, à l'aide de l'argument `-U_FORTIFY_SOURCE`.

L'option `-fstack-protector` connue sous le nom de SSP ("*Stack-Smashing Protector*" et autrefois connue sous le nom de ProPolice) est une option du compilateur GCC. Cette fonctionnalité consiste à générer une valeur aléatoire (canari) au démarrage du processus pour la placer dans la zone mémoire TLS ("`Thread Local Storage`") du processus. Cette zone n'est accessible que depuis le registre de segment `%gs` en mode utilisateur pour les applications Linux 32-bit et possède la valeur de référence du canari. Ce canari est vérifié dans chaque fonction qui contient un tampon de 8 octets minimum sur la pile. La taille de 8 octets est paramétrable à l'aide de l'argument `-param=ssp-buffer-size=N` lors de la compilation. Le mécanisme de protection de la fonction repose sur 2 étapes :

- dans le prologue de la fonction, le canari est stocké dans la pile juste avant l'adresse de retour de la fonction :

```
push ebp
mov ebp, esp
sub esp, 0x20
mov ebx, DWORD PTR [ebp+0xc]
mov eax, gs:0x14
mov DWORD PTR [esp+0x1c], eax
```

- dans l'épilogue de la fonction, le canari stocké dans la pile est comparé avec la valeur de référence dans la zone TLS `(gs:0x14)` pour vérifier que le canari n'a pas été écrasé lors d'un débordement de tampon pendant l'exécution de la fonction. Lorsque le canari sur la pile est modifié, la fonction ne retourne pas sur son adresse de retour (saved EIP) mais appelle la fonction `__stack_chk_fail` qui va afficher le message d'erreur `***stack smashing detected***` et terminer le processus :

```
mov edx, DWORD PTR [esp+0x1c]
xor edx, DWORD PTR gs:0x14
je fin_normale_de_la_fonction
call __stack_chk_fail
```

A titre anecdotique, le nom canari vient des mineurs qui emportaient autrefois avec eux un canari en cage. L'agitation du canari voire des signes de suffocation étaient caractéristiques d'un danger imminent.

L'option `-fstack-protector-all` permet d'ajouter le système de canari dans toutes les fonctions du programme et non plus seulement dans les fonctions qui contiennent des tampons de 8 octets minimum. Cette

option renforce la sécurité du programme mais le rend plus lent. En effet, pour chaque fonction, une routine qui permet de stocker le canari dans la pile est ajoutée dans chaque prologue de fonction, ainsi qu'une routine qui compare le canari avec sa valeur de référence dans chaque épilogue de fonction. Avec l'arrivée de GCC 4.9, un compromis a été fait entre `-fstack-protector-all` et `-fstack-protector` : il s'agit de `-fstack-protector-strong`. Cette option permet d'ajouter un canari seulement dans les fonctions contenant :

- des adresses de variable locales utilisées en tant qu'opérateur de droite dans les affectations ou en tant que paramètres dans les appels de fonction ;
- des variables locales de type tableaux ;
- des variables locales de type registre (`register int var = 0`).

L'utilisation de cette option constitue un compromis intéressant entre le renforcement de la sécurité et l'impact sur les performances. Elle peut être notamment utilisée pour compiler le noyau Linux depuis la version 3.14 grâce à l'option `CONFIG_CC_STACKPROTECTOR_STRONG`.

Le CERT-FR rappelle que la version 4.9 de GCC est encore une version de développement et qu'elle est disponible dans la version expérimentale de Debian. De plus, le CERT-FR recommande d'utiliser les protections de type SSP pour protéger les programmes nécessitant une protection renforcée.

- `-fstack-protector-strong` :
  http://www.outflux.net/blog/archives/2014/01/27/fstack-protector-strong/
- `FORTIFY_SOURCE` :
  https://idea.popcount.org/2013-08-15-fortify_source/

4 - Rappel des avis émis

Dans la période du 24 au 30 janvier 2014, le CERT-FR a émis les publications suivantes :

- CERTFR-2014-AVI-041 : Multiples vulnérabilités dans Apple iTunes
- CERTFR-2014-AVI-042 : Vulnérabilité dans Apple Pages
- CERTFR-2014-AVI-043 : Vulnérabilité dans Xen
- CERTFR-2014-AVI-044 : Vulnérabilité dans Huawei Eudemon8000E
- CERTFR-2014-AVI-045 : Multiples vulnérabilités dans Google Chrome
- CERTFR-2014-AVI-046 : Multiples vulnérabilités dans Pidgin
- CERTFR-2014-AVI-047 : Vulnérabilité dans MediaWiki

Gestion détaillée du document

31 janvier 2014 version initiale.