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 22 février 2016
N° CERTFR-2016-ACT-008

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2016-ACT-008

1 - Gestion des mots de passe des administrateurs locaux - Partie 2

Introduction

Dans le cadre de la gestion des comptes locaux des systèmes Windows (en particulier ceux des administrateurs locaux), il est possible d'utiliser les GPO de préférence. La méthode consiste à créer un compte local, à lui assigner un mot de passe puis à ajouter ce compte dans le groupe des Administrateurs locaux. Cependant, la méthode de stockage du mot de passe dans les fichiers des GPO présente des risques de sécurité, précédemment présentés dans le bulletin d'actualité CERTFR-2015-ACT-046. Ainsi, cette méthode est désormais désactivée par Microsoft au moyen du bulletin de sécurité MS14-025. Microsoft a publié en juillet 2015 un outil dénommé LAPS (Local Administrator Password Solution) qui permet de gérer automatiquement les mots de passe des comptes d'administrateurs locaux.

LAPS (Local Administrator Password Solution)

Préalablement à la mise en œuvre de LAPS, il est vivement recommandé de supprimer tous les comptes utilisateurs créés au moyen des GPO de préférence. En effet, garder les deux méthodes de gestion (par GPO et par LAPS) invalide les mots de passe stockés par LAPS dans l'annuaire Active Directory. L'outil LDAP est disponible sur le site de Microsoft, ainsi que la procédure d'installation. Dans son principe, LAPS permet de stocker de manière sécurisée le mot de passe des administrateurs locaux des systèmes Windows au sein de l'annuaire Active Directory, puis de procéder périodiquement à son renouvellement. Ceci permet d'obtenir des mots de passe uniques sur chaque poste pour les administrateurs locaux, évitant ainsi le rejeu des mots de passe ou des identifiants de postes en postes. De plus, il est possible de définir une politique de robustesse associée aux mots de passe ainsi générés.

Mise en œuvre sur le contrôleur de domaine

Il est nécessaire de procéder à une extension du schéma LDAP de l'Active Directory pour ajouter, aux objets de type `computer`, les attributs suivants :

- l'attribut `ms-Mcs-AdmPwd` qui contient le mot de passe du compte ;
- l'attribut `ms-Mcs-AdmPwdExpirationTime` qui renseigne la durée de validité du mot de passe.

Ces attributs sont marqués comme *confidential* dans le schéma de l'Active Directory. Ainsi, un utilisateur ayant des permissions de lecture (`READ_PROPERTY`) sur l'attribut doit également disposer du droit `CONTROL_ACCESS` pour le lire. Ceci permet, dans une configuration par défaut des droits, de n'autoriser l'accès qu'aux utilisateurs privilégiés de l'Active Directory. Pour étendre le schéma, il faut exécuter les commandes Powershell suivantes avec un compte autorisé à étendre le schéma :

```
Import-Module AdmPwd.PS
Update-AdmPwdADSchema
```

Il faut ensuite déléguer les droits de mise à jour des mots de passe aux ordinateurs membres du domaine :

```
Set-AdmPwdComputerSelfPermissions -OrgUnit 'Domain Computers'
```

Il est crucial de s'assurer que les permissions sur les objets de type `computer` n'autorisent l'accès à ces attributs qu'aux utilisateurs légitimes. Pour cela, il est nécessaire d'exécuter la commande suivante puis supprimer les droits superflus :

```
Find-AdmPwdExtendedRights -Identity 'Domain Computers'
```

Par défaut, seuls les administrateurs du domaine et l'entité `SYSTEM` ont des droits sur ces attributs. Il est possible de déléguer ces droits aux membres de groupes spécifiques, qui pourront légitimement récupérer et éventuellement modifier les mots de passe des Administrateurs locaux :

```
Set-AdmPwdReadPasswordPermission -Identity 'Domain Computers' -AllowedPrincipals "Help D
Set-AdmPwdReadPasswordPermission -Identity 'Servers' -AllowedPrincipals "Servers Admins"
```

Mise en œuvre sur les systèmes

Sur les systèmes Windows pour lesquels le compte administrateur local doit être géré par LAPS, il faut installer l'extension GPO (Client Site Group Policy Extension) `AdmPwd`. Cette extension, fournie par Microsoft, est installable au moyen d'un fichier MSI et peut donc être déployée par GPO.

Administration de LAPS

L'outil d'administration LAPS permet de lire le mot de passe de l'administrateur local d'un système sur lequel LAPS est appliqué. Il offre également la possibilité d'imposer un changement immédiat du mot de passe, ce qui est indispensable lorsque le mot de passe a été révélé ou utilisé par ailleurs. Exemple de commande PowerShell permettant de réinitialiser un mot de passe sur un ordinateur particulier :

```
Reset-AdmPwdPassword 'ComputerName'
```

Exemple de commande PowerShell permettant de lire le mot de passe d'un système donné :

```
Get-AdmPwdPassword -ComputerName 'computer'
```

LAPS mettant en œuvre des attributs Active Directory (`ms-Mcs-AdmPwd` et `ms-Mcs-AdmPwdExpirationTime`), il est également possible de les lire ou les modifier en utilisant l'éditeur d'attributs Microsoft ou tout autre produit compatible LDAP. Cependant, il faut veiller à ce que les communications soient correctement chiffrées.

Documentation

- https://support.microsoft.com/en-us/kb/2962486
- http://blogs.msdn.com/b/laps/archive/2015/06/19/laps-and-ms14-025.aspx
- http://www.microsoft.com/en-us/download/details.aspx?id=46899
- http://technet.microsoft.com/en-us/library/security/3062591.aspx
- http://blogs.msdn.com/b/laps/archive/2015/06/01/laps-and-password-storage-in-clear-text-in-ad.aspx

2 - Vulnérabilités dans glibc

Une vulnérabilité de type "dépassement de tampon" a été découverte par l'équipe de sécurité de Google. Cette vulnérabilité permettrait, en cas d'exploitation, l'exécution de code arbitraire à distance. La GNU C Library (glibc) est l'implémentation de la bibliothèque C standard pour le projet GNU. Toutes les versions de la glibc ultérieures à 2.9 sont affectées par cette faille de sécurité.
La vulnérabilité se trouve dans le code des fonctions `send_dg()` et `send_vc()` qui sont définies dans le module libnss_dns.so.2. Ces fonctions sont appelées par des fonctions de plus haut niveau telles que `getaddrinfo()`. Cette dernière permet d'envoyer une requête à un serveur DNS afin de résoudre un nom de domaine en une adresse IP et vice versa.

Analyse de la vulnérabilité CVE-2015-7547

Lorsque la fonction `getaddrinfo()` est appelée sans spécifier la famille d'adresse (via le flag "AF_UNSPEC"), le client DNS va envoyer deux requêtes en parallèle au serveur DNS : une requête de type A pour une adresse IPv4 et une requête de type AAAA pour IPv6.
Le client DNS réserve un espace mémoire de 2048 octets sur la pile (via la fonction `alloca()`) pour y stocker la réponse de la première requête. Si le bloc mémoire n'est pas rempli entièrement, le même espace est réutilisé pour sauvegarder la réponse de la deuxième requête.
S'il n'y a pas assez d'espace pour stocker cette réponse, un nouveau tampon de 65535 octets sera alors alloué sur le tas via la fonction `malloc()`.
C'est à cet endroit où se situe le code vulnérable. En effet, c'est la taille du premier tampon qui est mise à jour à la place de la taille du nouveau tampon. Voici l'état des pointeurs à ce moment-là :

- Si le bloc de 2048 octets est rempli entièrement, la taille disponible dans le premier tampon pour la deuxième réponse est à 0 ;
- le pointeur du tampon de la 2e réponse pointe vers le bloc alloué sur le tas ;
- la taille du buffer pour la première réponse et à 65535 à la place de 2048 ;
- la taille du nouveau tampon est à 0 à la place de 65535 ;
- le pointeur du tampon pour la 1re réponse pointe toujours sur le bloc de 2048 octets sur la pile.

Après la mise à jour des pointeurs, la fonction `recvfrom()` est appelée pour lire les données de la réponse de la deuxième requête, mais échoue car la taille du nouveau tampon est à 0, on essaie alors de lire 0 octet de la réponse. Cela provoque un nouvel appel à la fonction `send_dg()`. Cette fois, le calcul de l'espace disponible sera biaisé car il vaudra 65535 - la taille de la première réponse. Il sera possible de concevoir une réponse DNS spécifique pour que le bloc mémoire sur la pile soit réutilisé pour y stocker la deuxième réponse. Comme le bloc sur la pile fait en réalité 2048 octets, un attaquant dispose de 65535-2048 octets pour insérer un code d'exploitation.
Il peut y avoir différents vecteurs d'attaque, par exemple, une réponse DNS pourrait être altérée via une attaque par l'homme du milieu ou un attaquant pourrait prendre le contrôle d'un serveur DNS.

Recommandations

Il est recommandé de vérifier la version de glibc installée sur le système et d'appliquer le correctif de sécurité qui règle ces problèmes.

Documentation

- Entrée de blog de l'équipe Google Security

  https://googleonlinesecurity.blogspot.fr/2016/02/cve-2015-7547-glibc-getaddrinfo-stack.html
- Correctif de sécurité et détails sur la vulnérabilité

  https://sourceware.org/ml/libc-alpha/2016-02/msg00416.html
- Preuve de concept

  https://github.com/fjserna/CVE-2015-7547
- Alerte CERTFR-2016-AVI-066 du 17 février 2016

  http://cert.ssi.gouv.fr/site/CERTFR-2016-AVI-066/index.html

3 - Rappel des avis émis

Dans la période du 15 au 21 février 2016, le CERT-FR a émis les publications suivantes :

- CERTFR-2016-ALE-001-001 : Campagne de messages électroniques non sollicités de type Locky
- CERTFR-2016-AVI-065 : Multiples vulnérabilités dans les produits Cisco
- CERTFR-2016-AVI-066 : Vulnérabilité dans glibc
- CERTFR-2016-AVI-067 : Vulnérabilité dans Squid
- CERTFR-2016-AVI-068 : Vulnérabilité dans Google Chrome

Gestion détaillée du document

22 février 2016 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-2016-ACT-008`