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 mars 2014
N° CERTFR-2014-ACT-011

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2014-ACT-011

1 - Comptes de service en environnement AD (troisième partie) : nouveaux mécanismes Windows

Les services applicatifs Windows (ou plus simplement services) sont des programmes gérés par le SCM (« Service Control Manager »), démarrés en tâche de fond du système, même si aucun utilisateur n'est connecté. Ils assurent différentes fonctions, telles que la gestion du système, la mise à jour d'applications, etc. Comme tout processus, les services doivent s'exécuter sous un compte utilisateur qui est par nature un « compte de service » (au sens de la définition du premier article de cette série).

Jusqu'à Windows 2000, seuls l'entité `SYSTEM` (ou `LocalSystem`) ou un compte utilisateur (local au système ou d'un domaine) pouvaient être utilisés. Ces deux possibilités ont cependant des inconvénients. Premièrement, l'entité `LocalSystem` dispose d'énormément de droits et de privilèges sur le système et est généralement trop privilégiée pour les opérations demandées par le service. Lorsqu'un service s'exécute sous l'entité `LocalSystem`, aucun mot de passe n'est nécessaire pour démarrer le service. Si la machine est membre d'un domaine et que le service doit s'authentifier sur des ressources distantes, ce sont les authentifiants de la machine (c'est-à-dire ceux associés à la machine dans le domaine) qui sont utilisés si Kerberos est le protocole d'authentification mis en œuvre. Dans le cas contraire (par exemple avec NTLM), le service n'a pas de capacité d'authentification distante : il essaye une session d'authentification nulle, qui est généralement refusée.

Deuxièmement, un service s'exécutant sous un compte utilisateur nécessite une configuration particulière : le compte doit être créé et paramétré pour démarrer le service. En outre, la gestion du mot de passe associé est fastidieuse : celui-ci doit être renseigné lors de l'installation du service et est stocké en clair dans le système. Ainsi, le mot de passe est rarement changé et paramétré pour échapper aux politiques de gestion (`DONT_EXPIRE`).

Avec Windows XP, Microsoft a ajouté deux comptes de service dédiés : `LocalService` et `NetworkService`. Tout comme `LocalSystem`, ces comptes ne nécessitent pas de mot de passe. Cependant, ils sont nettement moins privilégiés que celui-ci. La grande différence entre ces deux comptes est le contexte en cas d'authentification distante. `NetworkService` s'authentifie avec les authentifiants de la machine (si celle-ci est membre d'un domaine) alors que `LocalService` n'a pas de capacité d'authentification distante.

Avec Windows Vista/2008, Microsoft a ajouté les fonctionnalités suivantes :

- un service peut demander à disposer d'un identifiant de sécurité propre (SID) dans son contexte de sécurité. Cet identifiant est associé au nom du service et est résolu sous le nom `NTSERVICE\nom_du_service`. Cet identifiant est utilisé pour restreindre les accès aux ressources utilisées par le service ;
- chaque service dispose d'un certain nombre de privilèges liés au contexte de sécurité du compte sous lequel il s'exécute. Un service peut demander à perdre certains de ces privilèges. Ce mécanisme est utilisé pour restreinte le plus finement possible les privilèges accordés à chaque service ;
- un service peut utiliser le mécanisme des *restricted SID* afin de perdre des droits, en particulier ceux associés aux entités `LocalSystem`, `NetworkService`, utilisateurs authentifiés, etc.

Avec Windows 7/2008R2, deux nouveaux mécanismes sont apparus. Le premier baptisé « compte virtuel » (*virtual Account*) permet d'exécuter un service sous l'identifiant de sécurité qui lui est associé (`NTSERVICE\nom_du_service`). Aucun mot de passe n'est nécessaire pour la configuration du service et les droits ou privilèges associés sont ceux accordés au compte virtuel du service (par défaut, très similaires à ceux d'un simple utilisateur). En cas d'authentification distante, ce sont les authentifiants de la machine qui sont utilisés. Ce mécanisme permet d'isoler plus facilement les services entre eux et est utilisé, par exemple, pour démarrer les *workers* IIS sous des entités distinctes. L'autre mécanisme est celui des « comptes de service gérés » (*standalone managed service account*). Il s'agit de comptes utilisateur du domaine de classe LDAP `msDS-ManagedServiceAccount` ayant un nom de la forme `DOMAINE\nom_du_compte$`. Une fois créés dans l'annuaire, ils sont assignés à une (et une seule) machine du domaine et peuvent alors être utilisés pour démarrer un service sur celle-ci. L'intérêt est que le mot de passe est géré par la machine à laquelle le compte a été assigné. Il est ainsi changé périodiquement (tous les 30 jours par défaut). Les droits et privilèges sont, comme pour les comptes virtuels, ceux accordés au compte. Enfin, en cas d'authentification distante, ce sont les authentifiants du compte qui sont utilisés (et non ceux de la machine).

Enfin Windows 8/2012 a vu l'apparition des comptes de service administrés de groupe (*group managed service accounts*). Ce mécanisme étend le fonctionnement des comptes de service gérés en adressant plusieurs de leurs limitations :

– ils peuvent être utilisés pour exécuter des tâches planifiées ;

– ils ne sont plus associés à un seul ordinateur et peuvent être utilisés sur plusieurs ordinateurs simultanément.

La gestion et la distribution des mots de passe de ces comptes sont alors assurées par un service KDS (*Key Distribution Service*). Si le nom et le fonctionnement de ces comptes sont identiques à ceux des comptes de service gérés, ils diffèrent par leur classe LDAP (`msDSGroupManagedServiceAccount`).

En conclusion, depuis Windows 2000 sont apparus de nombreux mécanismes permettant de gérer les comptes utilisés comme compte de service. Le CERT-FR recommande leur mise en œuvre afin d'éviter d'utiliser des comptes trop privilégiés ou dont le mot de passe n'expire jamais.

2 - Chiffrement des ordiphones

Les ordiphones supportent des mécanismes de chiffrement des données afin de protéger la confidentialité des données enregistrées sur l'appareil en cas de vol. Ces mécanismes s'appuient souvent sur l'utilisation d'un code de déverrouillage dont la complexité a un impact direct sur la sécurité des données chiffrées. Cependant, le chiffrement d'un ordiphone ne permet pas de se protéger contre une application malveillante. En effet, lorsque le volume est déverrouilé, les données sont accessibles sans difficulté.

Le chiffrement d'un ordiphone permet également l'effacement rapide des données : seule la clé utilisée est effacée, les données chiffrées devenant alors inexploitables. Il peut également protéger les données de l'utilisateur contre des attaques mettant en œuvre une récupération physique de la mémoire flash (dessoudage) : la protection de la clé étant assurée par le mot de passe utilisateur ou un composant matériel (TPM, . . .).

Les systèmes *Android*, *Apple iOS* et *Windows Phone* reposent sur des systèmes de chiffrement différents.

Android

Le chiffrement de la partition contenant les données de l'utilisateur peut être activé par l'utilisateur depuis la version 3.0 (tablettes) et 4.0 (smartphones). L'option se trouve dans le menu « Paramètres »/« Sécurité »/« Chiffrer le téléphone». L'utilisateur est alors contraint d'utiliser un code PIN ou un mot de passe qui lui seront demandés à chaque démarrage du périphérique. L'option de déverrouillage par schéma est alors désactivée. Le système de chiffrement repose sur le système *dm-crypt* utilisant l'algorithme AES-128-CBC.

iPhone

Le chiffrement (AES-256-CBC) du volume de données sur *iPhone* est activé par défaut et ne peut être désactivé. L'ensemble du processus est transparent pour l'utilisateur. Outre le chiffrement du volume (permettant l'effacement rapide), chaque fichier peut être chiffré avec une clé unique et protégé par le PIN ou le mot de passe de l'utilisateur. La protection choisie est du ressort de l'application pour ses propres données ou du ressort du système (mots de passe WiFi, VPN, etc.) et consiste à spécifier si l'accès aux données nécessite le déverrouillage du téléphone. Le PIN ou le mot de passe est alors utilisé lors des opérations de cryptographie.

Windows Phone

Le chiffrement sous *Windows Phone* 8 n'est pas activé par défaut. Il peut être activé en appliquant la politique de sécurité (*Exchange ActiveSync*) `RequireDeviceEncryption`. Il utilise la technologie *Bitlocker* (AES-128). Ce chiffrement est transparent pour l'utilisateur et ne nécessite pas l'utilisation d'un mot de passe ou d'un PIN (les clés étant protégées grâce à une puce *TPM* embarquée).

Conclusion et recommandations

Le CERT-FR recommande la mise en œuvre des mécanismes de chiffrement des ordiphones afin d'assurer la confidentialité des données stockées. Par ailleurs, il convient d'activer les mécanismes de verrouillage automatique des ordiphones après un court délai d'inactivité. En cas d'utilisation de mots de passe de déverrouillage, il est important de choisir des mots de passe suffisamment robustes.

Documentation

- Fonctionnement du chiffrement sur Android :
  https://source.android.com/devices/tech/encryption/android_crypto_implementation.html
- Guide de sécurité iOS - Février 2014 :
  http://images.apple.com/ipad/business/docs/iOS_Security_Feb14.pdf
- Panorama sur la sécurité de Windows Phone 8 :
  http://go.microsoft.com/fwlink/?LinkId=2666838

3 - Réduction des méthodes de contournement de l'ASLR sous Microsoft Windows

La technique de protection ASLR (« Adress Space Layout Randomization ») est un mécanisme de défense en profondeur introduit par Microsoft avec Windows Vista.

Utilisée conjointement avec la protection DEP (« Data Excecution Prevention »), elle permet d'augmenter la difficulté et les compétences nécessaires pour écrire des codes d'exploitation fiables. En effet, la disposition de façon aléatoire des différentes zones mémoires virtuelles d'un processus impacte le fonctionnement des attaques exploitant la technique de ROP (« Return-Oriented Programming »).

Depuis l'apparition de ce mécanisme, différentes méthodes de contournement ont été découvertes. On peut notamment citer :

- le chargement d'une bibliothèque n'ayant pas été compilée avec la prise en charge de la protection ASLR ;
- l'utilisation d'une vulnérabilité de type divulgation d'information permettant à l'attaquant d'obtenir des détails sur l'espace d'adressage utilisé par le processus.

Microsoft s'efforce, au fil de ses mises à jour, de réduire le champ de ces méthodes de contournement :

- par la suppression de l'ensemble des pointeurs de fonctions présents, à adresse fixe, dans l'espace mémoire « SharedUserData » partagé entre l'espace noyau et l'espace utilisateur (MS13-063) ;
- par la recompilation de bibliothèques, fournies avec des produits Microsoft, qui ne prenaient pas en charge la protection ASLR, par exemple :
  - la bibliothèque `HXDS.DLL` incluse dans Microsoft Office 2003 et 2010 (MS13-106),
  - la bibliothèque `VSAVB7RT.DLL` incluse dans Microsoft .Net (MS14-009).

La mise en place de ces améliorations permet d'empêcher l'exploitation de vulnérabilités récentes telles que la vulnérabilité CVE-2014-0324 (visant Microsoft Internet Explorer 8). En effet, l'exploitation de cette vulnérabilité repose sur la présence de la bibliothèque `HXDS.DLL` afin de générer une chaîne « ROP » permettant l'exécution de code préparant la mise en place de la charge utile.

Cependant il n'est pas possible pour Microsoft de modifier les bibliothèques tierces. Ainsi, lors de tentatives d'exploitation, il est fréquent de trouver des codes permettant le chargement de bibliothèques provenant d'autres éditeurs. Il a par exemple été vu dans un exemple de code d'exploitation de la vulnérabilité CVE-2014-0502 un code chargé de détecter la présence d'Oracle Java 1.6.x. Cette version embarque la bibliothèque `MSVCR71.DLL` qui n'est pas soumise à la protection ASLR.

Afin de contourner cette limitation il est possible d'utiliser l'outil EMET de Microsoft qui permet de forcer la protection ASLR (« Mandatory ASLR ») sur l'ensemble du système, y compris pour les bibliothèques qui n'ont pas

été compilées avec le support de cette protection. Lors du chargement d'une de ces bibliothèques par un processus, EMET va alors procéder à l'allocation de données à l'adresse de chargement préférée (champ «ImageBase» de la structure PE) de la bibliothèque afin de forcer le chargement de celle-ci à une adresse non prédictible. Les versions d'Internet Explorer 10 et 11 ainsi qu'Office 2013 utilisent le même mécanisme qu'EMET afin d'apporter la protection ASLR à l'ensemble des greffons et bibliothèques chargés par ces programmes.

Enfin, l'utilisation de systèmes 64 bits et d'un système d'exploitation récent (Microsoft Windows 7, 8 et 8.1) permet d'augmenter l'efficacité de la protection ASLR grâce à des améliorations apportées sur ces nouvelles versions du système d'exploitation. On peut notamment citer :

- l'utilisation d'un espace d'adressage mémoire supérieur à 4 Go afin de renforcer la disposition aléatoire des adresses utilisées ;
- l'application du placement aléatoire pour des zones mémoires allouées via des fonctions telles que « VirtualAlloc ».

Le CERT-FR recommande donc d'utiliser les versions les plus récentes du système d'exploitation Microsoft Windows ainsi que l'utilisation d'un matériel 64 bits. Il est par ailleurs recommandé d'installer l'outil EMET de Microsoft et d'utiliser les dernières versions d'Internet Explorer et d'Office.

Documentation

- Bulletin de sécurité Microsoft MS13-063 :
  https://technet.microsoft.com/fr-fr/security/bulletin/ms13-063
- Bulletin de sécurité Microsoft MS13-106 :
  https://technet.microsoft.com/fr-fr/security/bulletin/ms13-106
- Bulletin de sécurité Microsoft MS14-009 :
  https://technet.microsoft.com/fr-fr/security/bulletin/ms14-009
- Articles de Microsoft sur les améliorations apportées sur l'ASLR :
  - http://blogs.technet.com/b/srd/archive/2013/12/11/software-defense-mitigating-common-exploitation–exploitation-techniques.aspx
  - http://blogs.technet.com/b/srd/archive/2014/03/11/when-aslr-makes-the-difference.aspx
- Articles du CERT-FR sur l'ASLR :
  - http://www.cert.ssi.gouv.fr/site/CERTA-2013-ACT-033/
  - http://www.cert.ssi.gouv.fr/site/CERTA-2013-ACT-042/
  - http://www.cert.ssi.gouv.fr/site/CERTA-2013-ACT-052/

4 - Rappel des avis émis

Dans la période du 07 au 13 mars 2014, le CERT-FR a émis les publications suivantes :

- CERTFR-2014-AVI-107 : Multiples vulnérabilités dans le noyau Linux d'Ubuntu
- CERTFR-2014-AVI-108 : Vulnérabilité dans Huawei eSpace Meeting
- CERTFR-2014-AVI-109 : Vulnérabilité dans IBM WPAR ftp pour AIX
- CERTFR-2014-AVI-110 : Multiples vulnérabilités dans Wireshark
- CERTFR-2014-AVI-111 : Multiples vulnérabilités dans Apache Struts
- CERTFR-2014-AVI-112 : Multiples vulnérabilités dans Oracle Solaris
- CERTFR-2014-AVI-113 : Vulnérabilité dans Squid
- CERTFR-2014-AVI-114 : Multiples vulnérabilités dans Google Chrome
- CERTFR-2014-AVI-115 : Multiples vulnérabilités dans Adobe Flash
- CERTFR-2014-AVI-116 : Multiples vulnérabilités dans les produits Apple
- CERTFR-2014-AVI-117 : Multiples vulnérabilités dans VMware vSphere
- CERTFR-2014-AVI-118 : Multiples vulnérabilités dans Microsoft Internet Explorer
- CERTFR-2014-AVI-119 : Vulnérabilité dans Microsoft DirectShow
- CERTFR-2014-AVI-120 : Vulnérabilité dans Microsoft Silverlight
- CERTFR-2014-AVI-121 : Multiples vulnérabilités dans le noyau de Microsoft Windows
- CERTFR-2014-AVI-122 : Vulnérabilité dans le protocole Microsoft Security Account Manager Remote
- CERTFR-2014-AVI-123 : Multiples vulnérabilités dans Juniper

– CERTFR-2014-AVI-124 : Vulnérabilité dans Adobe Shockwave Player
– CERTFR-2014-AVI-125 : Multiples vulnérabilités dans Asterisk

Durant la même période, les publications suivantes ont été mises à jour :
– CERTFR-2014-ALE-001-002 : Vulnérabilité dans Microsoft Internet Explorer (fermeture de l'alerte, suite à la diffusion du correctif par l'éditeur.)
– CERTFR-2014-AVI-104-001 : Vulnérabilité dans Nginx (mise à jour systèmes affectés)

Gestion détaillée du document

14 mars 2014 version initiale.