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 11 avril 2016
N° CERTFR-2016-ACT-015

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2016-ACT-015

1 - Risques liés à la configuration par défaut de WSUS

Cet article présente une attaque permettant de prendre le contrôle d'une machine Windows à distance dans un environnement où *Windows Server Update Service* (WSUS) est utilisé avec sa configuration par défaut. Nous verrons qu'il est possible de se protéger contre cette menace en configurant correctement WSUS.

Aperçu de WSUS

WSUS est le service applicatif permettant aux administrateurs Windows d'un parc de gérer la distribution des mises à jour Microsoft (tous les produits édités par Microsoft). Pour ce faire, le serveur WSUS fait office d'intermédiaire entre le service *Windows Update* public de Microsoft et les produits du système d'information à mettre à jour.

Pour installer une mise à jour, le client *Windows Update* récupère, auprès du serveur WSUS :

- le fichier de mise à jour (signé par une autorité de certification Microsoft) ;
- des métadonnées, indiquant notamment comment appliquer la mise à jour en question.

Configuration par défaut de WSUS

Dans sa configuration par défaut, les communications WSUS sont transmises, en clair, via le protocole HTTP. Sans protection supplémentaire, ce protocole est connu pour être vulnérable aux attaques de type `homme au milieu`. Dans le cas présent comme les fichiers de mise à jour doivent être signés par Microsoft, la potentielle modification en chemin d'une mise à jour par un attaquant sera détectée par le client Windows Update et l'installation sera alors bloquée.

Néanmoins, les métadonnées de la mise à jour ne sont pas authentifiées par le client. Elles permettent notamment d'indiquer au client Windows Update comment appliquer la mise à jour. Ainsi, il est possible d'exécuter le fichier de mise à jour (signé Microsoft) avec des arguments spécifiés dans les métadonnées (pour rappel: non signés donc non authentifiés). Ces mises à jour sont exécutées avec les privilèges les plus élevés (ceux du compte `NT AUTHORITY\SYSTEM`).

En conséquence, s'il existe un fichier légitime (signé par Microsoft) dont les arguments peuvent être utilisés pour exécuter des commandes arbitraires, alors un attaquant étant en mesure de modifier les données WSUS à destination d'une machine cliente peut en prendre le contrôle total. Il s'avère que l'utilitaire *PsExec* de la suite *Sysinternals* répond à tous ces critères.

Pour résumer, une personne malintentionnée ayant la capacité de se positionner en *homme du milieu* sur un réseau d'une organisation peut prendre le contrôle total des autres machines avec un scénario comme suit :

1. interception des communications entre une machine cliente et le serveur WSUS. Cela peut, par exemple, être obtenu par injection de fausses réponses *Web Proxy Auto-Discovery* (WPAD) ou encore par l'utilisation d'ARP *spoofing* ;

2. lorsqu'une machine cliente communique avec WSUS, ajout d'une mise à jour malveillante contenant PsExec comme fichier de mise à jour et des arguments arbitraires à exécuter dans les métadonnées non signées.

Sécuriser WSUS

Pour se protéger contre cette attaque, il est nécessaire de configurer le serveur WSUS et les clients pour qu'ils utilisent HTTPS comme protocole de transport WSUS. Le protocole WSUS sera alors implicitement chiffré et authentifié. Microsoft documente de façon détaillée les étapes de mise en oeuvre de cette configuration [1].

Identifier les machines vulnérables

Toute machine Windows configurée pour accéder à son serveur WSUS via HTTP est potentiellement vulnérable. Il est possible de vérifier la configuration d'un poste client en consultant les clés de registre :

1. `HKLM\Software\Policies\Microsoft\Windows\WindowsUpdate` : la valeur `WUServer` contient l'adresse du serveur WSUS. Si cette adresse ne commence pas par https://, la machine est potentiellement vulnérable ;
2. `HKLM\Software\Policies\Microsoft\Windows\WindowsUpdate\AU` : si la valeur `UseWUServer` est à 0, l'adresse spécifiée par `WUServer` est ignorée, si elle est à 1, l'adresse spécifiée par `WUServer` est utilisée.

Documentation

1 Configurer l'utilisation de SSL par WSUS :
https://technet.microsoft.com/library/hh852346.aspxbkmk_3.5.ConfigSSL

2 Paul Stone, Alex Chapman, *WSUSpect Compromising the Windows Enterprise via Windows Update*, Black Hat USA 2015, août 2015 :
https://www.blackhat.com/docs/us-15/materials/us-15-Stone-WSUSpect-Compromising-Windows-Enterprise-Via-Windows-Update-wp.pdf

2 - Neutralisation des comptes de l'Active Directory

Dans un annuaire, les comptes dormants correspondent à des comptes utilisateur ou machine, non désactivés qui ne se sont pas authentifiés depuis plusieurs mois, voire plusieurs années. Ces comptes dormants sont soit des comptes légitimes rarement utilisés, soit des comptes obsolètes, ces derniers devant faire l'objet d'un traitement particulier.

Deux critères peuvent être utilisés pour énumérer les comptes dormants dans un annuaire Active Directory :

– les comptes dont le mot de passe est assujetti à la politique de mots de passe du domaine (fanion `ADS_UF_DONT_EXPIRE_PA` non positionné dans la propriété `userAccountControl`) et dont la date de dernier changement (propriété `pwdLastSet`) est supérieure à celle de la politique de renouvellement des mots de passe ;
– les comptes n'ayant pas réalisé une authentification auprès du domaine depuis plusieurs mois (propriété `LastLogonTimestamp`). Attention, cette propriété n'est mise à jour que si le niveau de fonctionnalité du domaine est au moins positionné à Windows 2003.

Sont considérés comme obsolètes des comptes dormants dont l'existence dans le domaine n'est plus justifiée.

La présence de comptes obsolètes dans l'Active Directory peut s'expliquer par le départ ou le changement d'affectation d'un utilisateur, la suppression d'une application ou la mise au rebut d'une machine, le tout en l'absence de politique de gestion des comptes (technique ou organisationnelle).

Les comptes obsolètes peuvent donner des accès à des personnes n'en ayant plus besoin (faisant suite à un départ par exemple), ce qui est d'autant plus préjudiciable si ces comptes sont privilégiés.

Il est donc nécessaire de s'assurer que les comptes obsolètes, que ce soit des comptes utilisateur ou des comptes de machine, ne puissent plus être utilisés. La suppression de ces comptes pourrait répondre à ce besoin. Cependant, il ne serait plus possible de résoudre l'identifiant associé au compte supprimé. Ceci engendrerait une perte de traçabilité sur certains éléments (membres de groupes, droits positionnés sur les fichiers, etc.).

La simple désactivation des comptes permet en revanche de conserver cette traçabilité, mais ne permet pas de garantir qu'un utilisateur suffisamment privilégié ne puisse réactiver ces comptes et bénéficier des droits associés.

Ainsi, il convient de privilégier la neutralisation des comptes obsolètes, dont la procédure doit être la suivante :

- suppression de l'appartenance du compte à tous ses groupes ;
- changement du mot de passe associé au compte. Pour ce faire, il est recommandé de positionner le fanion ADS_UF_SMARTCARD_REQUIRED dans la propriété userAccountControl qui garantit un mot de passe aléatoire ;
- éventuellement, déplacement du compte dans une OU dédiée ;
- éventuellement, mise à jour du champ description du compte afin d'indiquer le contexte de désactivation (date, raison, etc.).
- désactivation du compte.

L'ANSSI recommande donc la méthode de neutralisation par rapport à celle de la suppression et de la simple désactivation. Celle-ci apporte les mêmes avantages que la suppression tout en conservant la traçabilité offerte par la simple désactivation.

3 - Rappel des avis émis

Dans la période du 04 au 10 avril 2016, le CERT-FR a émis les publications suivantes :

- CERTFR-2016-ALE-002 : Vulnérabilité dans Adobe Flash Player
- CERTFR-2016-AVI-112 : Multiples vulnérabilités dans Squid
- CERTFR-2016-AVI-113 : Multiples vulnérabilités dans Google Android (Nexus)
- CERTFR-2016-AVI-114 : Multiples vulnérabilités dans le noyau Linux d'Ubuntu
- CERTFR-2016-AVI-115 : Multiples vulnérabilités dans les produits Cisco
- CERTFR-2016-AVI-116 : Multiples vulnérabilités dans Adobe Flash Player

Gestion détaillée du document

11 avril 2016 version initiale.