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 24 novembre 2014
N° CERTFR-2014-ACT-047

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2014-ACT-047

1 - Vulnérabilité impactant Kerberos

Le 18 novembre 2014, Microsoft a publié un correctif hors cycle sur une vulnérabilité impactant le composant Kerberos (CVE-2014-6324). Le CERT-FR a publié le soir même l'alerte CERTFR-2014-ALE-011 pour prévenir des risques liés à l'exploitation de cette vulnérabilité.

Selon Microsoft, un attaquant pourrait exploiter cette vulnérabilité afin d'élever ses privilèges sur une forêt Active Directory. La vulnérabilité permettrait à utilisateur non privilégié de passer Administrateur du domaine. La seule contrainte est de pouvoir contacter le KDC (Key Distribution Center) et de connaître un compte utilisateur de l'infrastructure attaquée.

Microsoft précise que cette vulnérabilité est utilisée dans le cadre d'attaques ciblées. Cette mise à jour est effectuée en dehors des cycles classiques de publication Microsoft, ce qui confirme la criticité de ce correctif. Le CERT-FR recommande l'application de ce correctif de sécurité dès que possible.

Documentation

- https://technet.microsoft.com/fr-fr/library/security/ms14-068.aspx
- http://www.cert.ssi.gouv.fr/site/CERTFR-2014-ALE-011
- http://www.cert.ssi.gouv.fr/site/CERTFR-2014-AVI-489

2 - Retour d'expérience sur le changement du mot de passe de *krbtgt*

Rappels

Dans le bulletin d'actualité CERTFR-2014-ACT-032, le CERT-FR évoquait le rôle du compte `krbtrgt` dans les annuaires Active Directory et mettait en garde contre les conséquences liées à l'absence de changement du mot de passe de ce compte. Une procédure de changement du mot de passe de compte était détaillée dans le bulletin.

Depuis, le CERT-FR a été informé d'un cas de dysfonctionnement suite au changement du mot de passe du compte `krbtgt`. Il apparaît que le changement de ce mot de passe, en présence de contrôleurs de domaine sous Windows Server 2003, ne doit être entrepris que sous certaines conditions.

En revanche, pour les architectures dont les contrôleurs de domaine fonctionnent tous sous Windows Server 2008 ou supérieur, la procédure reste inchangée. Le double changement peut être entrepris, après qualification, tel que décrit dans le bulletin d'actualité CERTFR-2014-ACT-032.

Le CERT-FR rappelle cependant l'intérêt de l'opération de changement du mot de passe du compte `krbtgt` du point de vue de la sécurité. Par ailleurs, le processus de migration des contrôleurs de domaine fonctionnant encore sous Windows Server 2003 vers des versions plus récentes doit être planifié et exécuté, la fin de support de ce système étant fixée par Microsoft au 14 juillet 2015.

Utilisation des clés K_KDC

Le compte `krbtgt` est un compte utilisateur servant de support de stockage, dans ses attributs, aux clés des centres de distribution des tickets Kerberos (appelées clés K_KDC par la suite).

Ces clés sont utilisées dans deux cas. Le premier concerne le chiffrement des parties protégées des tickets de type TGT (ticket-granting ticket). Ces tickets sont récupérés par les clients auprès des contrôleurs de domaine et doivent être présentés à nouveau aux contrôleurs de domaine pour demander des tickets de service. Lorsque le mot de passe du compte `krbtgt` est changé, et par là même les clés K_KDC, les contrôleurs de domaine tentent de déchiffrer les TGT avec les clés actuelles, mais également avec les clés reposant sur la génération antérieure du mot de passe. Le changement du mot de passe du compte `krbtgt` ne pose, dans ce cas, aucun problème, y compris pour des contrôleurs de domaine sous Windows Server 2003.

Le deuxième cas d'utilisation des clés K_KDC est lié à la génération des signatures des données d'autorisation (appelées PAC pour *Privilege Account Certificate*) contenues dans les tickets. Dans certains cas, détaillés ci-dessous, lorsqu'un service reçoit un ticket de service, il sollicite un contrôleur de domaine pour valider la signature de la PAC contenue dans le ticket présenté. Avec des contrôleurs de domaine sous Windows Server 2008 et ultérieurs, la validation fonctionne correctement, même lorsque le mot de passe du compte `krbtgt` vient de changer. En revanche, les contrôleurs de domaine sous Windows Server 2003 ne valident la signature de la PAC qu'au moyen du mot de passe courant du compte `krbtgt`. Si celui-ci vient à changer, les signatures des PAC contenues dans les tickets Kerberos ne peuvent alors plus être validées, ce qui entraîne un échec de la validation de la signature et par conséquent un échec de l'authentification du client.

En fonction des couches applicatives utilisées, cet échec peut entraîner un dysfonctionnement dont la remédiation dépend de l'application (reprise de l'authentification, purge des tickets Kerberos, redémarrage, etc.). Dans tous les cas observés et envisageables, un redémarrage des postes clients ou des serveurs rétablira le fonctionnement nominal de l'application.

Si des contrôleurs de domaine Windows Server 2003 sont présents, il convient donc de déterminer si une validation de signature de la PAC est réalisée. Dans l'affirmative, il est nécessaire de prendre des dispositions lors de l'opération de changement du mot de passe de `krbtgt` afin de traiter l'échec de l'authentification si les couches applicatives ne le gèrent pas elles-mêmes (désactivation temporaire de la signature).

Conditions de validation de la signature de la PAC

La validation est conditionnée par le contexte de sécurité du processus du service concerné par l'authentification et par la version du système d'exploitation associé.

Windows Server 2000 et Windows XP : la signature de la PAC n'est pas effectuée lorsque le processus du service s'exécute sous le compte LocalSystem ou avec un compte disposant du privilège `SeTcbPrivilege`.

Windows Server 2003 : la signature de la PAC n'est pas effectuée lorsque le processus du service s'exécute sous le compte LocalSystem, NetworkService ou avec un compte disposant du privilège `SeTcbPrivilege`.

Windows Server 2003 Service Pack 1 : la signature de la PAC n'est pas effectuée lorsque le processus du service s'exécute sous le compte LocalSystem, NetworkService, LocalService ou avec un compte disposant du privilège `SeTcbPrivilege`.

Windows Server 2003 Service Pack 2 : la signature de la PAC n'est pas effectuée lorsque :

- le processus du service s'exécute sous le compte LocalSystem, NetworkService, LocalService ou avec un compte disposant du privilège `SeTcbPrivilege` ;
- le processus du service s'exécute comme un service Windows (hors contexte ci-dessus) et la clé de registre `ValidateKdcPacSignature` est positionnée à 0 (clé positionnée à 1 par défaut sous ce système).

Windows Server 2008, Windows Vista et ultérieurs : les conditions sont identiques à celles pour Windows Server SP2 sauf que la clé `ValidateKdcPacSignature` est, par défaut, positionnée à 0.

Il faut noter que la majorité des services rentrent dans les cas ci-dessus (partage de fichiers, services classiques de Windows, etc.). Cependant, dans tous les autres cas, la validation de la signature de la PAC est systématique et ne peut être désactivée. C'est en particulier le cas pour les applications pools de IIS ou les serveurs COM+ ou DCOM.

3 - Bonnes pratiques de stockage des mots de passe

Le CERT-FR constate régulièrement dans le cadre de ses missions que les règles de construction de mots de passe robustes et le stockage de ceux-ci de manière sécurisée ne sont pas toujours respectées, notamment en raison de la complexité de mise en œuvre et de suivi que cela impose à l'utilisateur.

Afin de réduire cette complexité, il est conseillé d'utiliser des solutions logicielles, nombreuses sur le marché, qui permettent non seulement de construire des mots de passe uniques et robustes, mais également de les stocker de manière chiffrée et sécurisée.

Parmi ces solutions, KeePass est un logiciel libre qui a été évalué par l'ANSSI dans le cadre d'une Certification de Sécurité de Premier Niveau (CSPN). La CNIL a publié une fiche pratique sur l'utilisation de ce logiciel.

Le CERT-FR recommande également la lecture et la mise en œuvre du guide publié par l'ANSSI sur les recommandations de sécurité relatives aux mots de passe (DAT-NT-001/ANSSI/SDE/NP).

Documentation

- Certificat CSPN KeePass :
  http://www.ssi.gouv.fr/fr/produits-et-prestataires/produits-certifies-cspn/certificat_cspn_2010_07.html
- Note ANSSI relative aux mots de passe :
  http://www.ssi.gouv.fr/IMG/pdf/NP_MDP_NoteTech.pdf
- Fiche pratique CNIL :
  http://www.cnil.fr/documentation/fiches-pratiques/fiche/article/securite-comment-construire-un-mot-de-passe-sur-et-gerer-la-liste-de-ses-codes-dacces/

4 - Rappel des avis émis

Dans la période du 17 au 23 novembre 2014, le CERT-FR a émis les publications suivantes :

- CERTFR-2014-ALE-011 : Vulnérabilité de l'implémentation Kerberos dans Microsoft Windows
- CERTFR-2014-AVI-484 : Multiples vulnérabilités dans les produits Huawei
- CERTFR-2014-AVI-485 : Multiples vulnérabilités dans Moodle
- CERTFR-2014-AVI-486 : Multiples vulnérabilités dans Xen
- CERTFR-2014-AVI-487 : Multiples vulnérabilités dans les produits Apple
- CERTFR-2014-AVI-488 : Multiples vulnérabilités dans Google Chrome
- CERTFR-2014-AVI-489 : Vulnérabilité de l'implémentation Kerberos dans Microsoft Windows
- CERTFR-2014-AVI-490 : Multiples vulnérabilités dans Drupal
- CERTFR-2014-AVI-491 : Vulnérabilité dans le smartphone P7 Huawei
- CERTFR-2014-AVI-492 : Vulnérabilité dans Xen

Durant la même période, les publications suivantes ont été mises à jour :

- CERTA-2005-INF-003-016 : Les systèmes et logiciels obsolètes (Actualisation et mise à jour des versions de tous les systèmes et de logiciels.)
- CERTA-2005-INF-003-016 : Les systèmes et logiciels obsolètes (Actualisation et mise à jour des versions de tous les systèmes et de logiciels.)

Gestion détaillée du document

24 novembre 2014 version initiale.