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 06 juin 2016
N° CERTFR-2016-ACT-023

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2016-ACT-023

1 - Attaque par l'homme du milieu sur KeePass 2

KeePass est un gestionnaire de mots de passe permettant de stocker l'ensemble de ses mots de passe dans un fichier chiffré qui sera accessible via une clé maîtresse.

L'implémentation de la vérification des mises à jour au sein de KeePass ne respecte pas les règles d'hygiène de la sécurité informatique. En effet, cette vérification est faite via une requête HTTP, la communication entre le gestionnaire de mot de passe et le serveur de mise à jour est donc faite de manière non chiffrée et non signée.
Il est donc possible pour un attaquant, via une attaque par l'homme du milieu, d'intercepter et de modifier ces requêtes à la volée afin de rediriger l'utilisateur vers une page de téléchargement malveillante.

Ce problème d'implémentation a un numéro de CVE (CVE-2016-5119) et affecte toutes les versions de KeePass 2 jusqu'à la version 2.33.

Recommandations

Le développeur de KeePass, Dominik Reichl, a annoncé que la vulnérabilité ne sera pas corrigée à cause des pertes de revenues via les régies de publicités engendrées par le passe d'HTTP en HTTPS. Il est donc recommandé de désactiver les mises à jour automatiques pour ce logiciel et réaliser les mises à jour manuellement.

De manière générale, et comme précisé dans le bulletin d'actualité CERTFR-2014-ACT-047 (section « Bonnes pratiques de stockage des mots de passe »), le CERT-FR recommande l'utilisation d'un gestionnaire de mots de passe afin de construire des mots de passe uniques et robustes et de les stocker de manière sécurisée.

Mise à jour du 14 juin 2016 : A partir de la version 2.34 de Keepass, les mise à jour sont désormais signées (RSA-4096/SHA-512) et transmises par un canal HTTPS, ce qui corrige la vulnérabilité décrite ci-dessus.

Documentation

- Détails sur la vulnérabilité
  https://bogner.sh/2016/03/mitm-attack-against-keepass-2s-update-check/
- Bulletin d'actualité CERTFR-2014-ACT-047
  http://cert.ssi.gouv.fr/site/CERTFR-2014-ACT-047/
- Avis CERTFR-2016-AVI-200
  http://cert.ssi.gouv.fr/site/CERTFR-2016-AVI-200/

2 - Guide de référence des évènements d'audit sous Windows

Sous Windows, toutes les opérations liées à la sécurité peuvent être tracées via des évènements d'audit de sécurité générés par le fournisseur « Microsoft-Windows-Security-Auditing ». Ces évènements obéissent aux critères suivants :

- ils ne peuvent être générés que par le système ;

– ils sont conservés dans le journal Windows « Sécurité » qui n'est accessible en lecture qu'aux membres des groupes locaux « Administrateurs » et « Lecteurs des journaux d'évènements » ;
– ils sont générés suivant une politique de journalisation définie dans la stratégie locale de sécurité.

La politique de journalisation d'un système Windows peut-être définie et consultée au moyen de l'éditeur graphique `secpol.msc` (Configuration avancée de la stratégie d'audit) ou au moyen de l'outil en ligne de commande `auditpol.exe`.

Depuis Vista, tous les évènements d'audit sont associés à une sous-catégorie d'audit (par exemple « Ouvrir la session »). Celle-ci définit si les évènements associés doivent être générés en cas de succès ou d'échec. Ces sous-catégories sont regroupées en catégories (par exemple « Ouvrir la session » appartient à la catégorie « Ouverture/Fermeture de session »). La commande `auditpol /get /category:*` permet d'obtenir la politique associée à toutes les sous-catégories.

Jusqu'à présent, il était difficile de connaître tous les évènements pouvant être émis, leur description ainsi que leur sous-catégorie d'audit associée. Microsoft a publié, le 17 mai 2016, un document baptisé « Windows 10 and Windows Server 2016 security auditing and monitoring reference » (cf. Documentation). Celui-ci recense et décrit tous les évènements liés aux audits de sécurité des systèmes Windows. Même si ce document est spécifique à Windows 10 et Windows Server 2016, la grande majorité des informations contenues est applicable aux systèmes Vista et ultérieurs. Pour chaque évènement, sont ainsi décrits :

– le numéro de l'évènement ;
– la sous-catégorie d'audit associée ;
– la politique par défaut (succès ou échec) ;
– la volumétrie attendue ;
– le message de l'évènement.

Ce document est particulièrement utile pour définir une politique de journalisation et pour connaitre la définition de tous les évènements dans le cadre d'un traitement des journaux Windows. Pour rappel, l'ANSSI recommande une politique d'audit applicable à tous les systèmes Windows (cf. Documentation - Annexe II du guide des « recommandations de sécurité relative à Active Directory »).

Documentation

– « Windows 10 and Windows Server 2016 security auditing and monitoring reference » par Microsoft
https://www.microsoft.com/en-us/download/details.aspx?id=52630
– « Recommandations de sécurité relatives à Active Directory » par l'ANSSI
http://www.ssi.gouv.fr/guide/recommandations-de-securite-relatives-a-active-directory/

3 - Rappel des avis émis

Dans la période du 30 mai au 05 juin 2016, le CERT-FR a émis les publications suivantes :

– CERTFR-2016-AVI-183 : Vulnérabilité dans Citrix NetScaler Gateway
– CERTFR-2016-AVI-184 : Vulnérabilité dans Citrix Studio
– CERTFR-2016-AVI-185 : Vulnérabilité dans Nginx
– CERTFR-2016-AVI-186 : Multiples vulnérabilités dans le noyau linux d'Ubuntu
– CERTFR-2016-AVI-187 : Multiples vulnérabilités dans les produits Cisco
– CERTFR-2016-AVI-188 : Multiples vulnérabilités dans Google Chrome
– CERTFR-2016-AVI-189 : Multiples vulnérabilités dans Xen

Gestion détaillée du document

06 juin 2016 version initiale.
14 juin 2016 Annonce de Keepass 2.34.