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 juillet 2014
N° CERTFR-2014-ACT-028

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2014-ACT-028

1 - Retour sur la vulnérabilité DPAPI

Depuis quelques jours, plusieurs sites Internet relaient une information concernant une vulnérabilité dans le mécanisme DPAPI de Windows. Cet article se propose de résumer les faits techniques et de déterminer les conséquences pour les utilisateurs et administrateurs.

DPAPI est un mécanisme de protection de secrets des utilisateurs apparu avec Windows 2000 en remplacement du Protected Storage (*Pstore*). Il est très largement utilisé pour la protection des mots de passe de messagerie, des mots de passe réseau, des clés privées associées aux certificats numériques, etc.

Le fonctionnement de DPAPI est détaillé par Microsoft dans un article de la documentation MSDN.

Pour simplifier, DPAPI protège des données en les chiffrant par un ensemble de clés qui, au final, sont protégées par une clé symétrique dérivée à partir du mot de passe de l'utilisateur.

Sous Windows 2000, l'algorithme MD4 était utilisé pour la dérivation du mot de passe. Or MD4 est également l'algorithme utilisé pour calculer les empreintes des mots de passe aux formats NTLM (*hash NTLM*). Dans ce scénario, si un attaquant arrive à récupérer les empreintes contenues dans une base de comptes (locale à une machine ou d'un annuaire Active Directory), les clés DPAPI (stockées dans le profil utilisateur sur le disque dur) et les secrets protégés (dans la grande majorité des cas également stockés dans le profil utilisateur), il est en mesure de déchiffrer ces secrets. Pour cela, il utilise l'empreinte MD4 (c'est-à-dire l'empreinte NTLM), qui lui permet de déchiffrer les clés DPAPI, puis les secrets protégés par ces clés.

Depuis Windows XP, SHA-1 a remplacé MD4 dans DPAPI. Le scénario décrit ci-dessus ne fonctionne alors plus car il n'est plus possible de déchiffrer les clés DPAPI à partir des empreintes NTLM. En effet, un accès physique à la machine ne permet plus de déchiffrer les secrets : l'empreinte SHA-1, utilisée pour chiffrer les clés DPAPI, n'est présente dans la mémoire du processus LSASS que lorsqu'un utilisateur est authentifié sur une machine.

La vulnérabilité récemment annoncée concerne les comptes de domaine pour lesquels, contrairement aux comptes locaux, DPAPI n'utilise pas SHA-1, mais toujours MD4. Ainsi, si un attaquant arrive à compromettre un annuaire Active Directory, il sera en mesure de déchiffrer les secrets DPAPI de tous les utilisateurs du domaine.

Ceci amène trois réflexions. Premièrement, l'attaque nécessite d'obtenir le plus haut niveau de droit sur au moins un contrôleur de domaine, afin de récupérer les empreintes NTLM dans la base des comptes de l'Active Directory. Or lorsqu'un attaquant récupère toute cette base, il obtient un contrôle total sur le système d'information. Il est donc en mesure de prendre contrôle de tous les postes de travail et pourrait récupérer les secrets par d'autres moyens (par exemple : *keylogger*, *hooking* de fonctions, etc.). La méthode utilisant les empreintes NTLM est cependant immédiate.

Deuxièmement, l'utilisation de l'algorithme MD4 pour les comptes domaine est rendue nécessaire dans certains cas. Par exemple, lorsqu'un utilisateur s'authentifie par carte à puce, il ne saisit aucun mot de passe. Le système ne peut donc pas générer d'empreinte SHA-1. La seule empreinte disponible est l'empreinte NTLM (c'est-à-dire celle au format MD4) qui est transmise par le contrôleur de domaine vers la session du client au moyen des extensions PKINIT de Kerberos.

Enfin, DPAPI inclut nativement un mécanisme de recouvrement pour les comptes de domaine (voir la section *Key Backup and Restoration in DPAPI* du document de présentation de DPAPI de Microsoft). En effet, lorsqu'un compte de domaine protège des secrets, via DPAPI, la clé de chiffrement du secret est également chiffrée, pour séquestre, avec la partie publique du bi-clé de sauvegarde DPAPI du domaine (cette clé est située dans le conteneur System de l'annuaire sous les entrées `BCKUPKEY_X`). La compromission de la base des comptes de l'annuaire permet donc structurellement à un attaquant de récupérer la partie privée du bi-clé de sauvegarde DPAPI. Il est alors en mesure de recouvrer tous les secrets DPAPI des comptes du domaine. Dans ce cas, l'utilisation de SHA-1 au lieu de MD4 pour les comptes de domaine ne change rien. Le recouvrement DPAPI, qui n'est pas désactivable, est nécessaire dans certains cas, tels que l'inaccessibilité du profil utilisateur (changement de poste ou perte du profil) ou lorsque le mot de passe d'un utilisateur est réinitialisé par un administrateur.

Les annonces récentes sur une vulnérabilité de DPAPI sont donc à relativiser. Elles nécessitent la compromission de la base des comptes d'un Active Directory et ne changent en rien la situation actuelle due au mécanisme de recouvrement.

Elles rappellent cependant la nécessité absolue de protéger la base des comptes de l'Active Directory. En effet, outre les graves conséquences induites par une compromission de cette base, celles engendrées par la récupération des secrets DPAPI des utilisateurs du domaine sont également à prendre en compte.

Documentation

- PStore :
  http://msdn.microsoft.com/en-us/library/bb432403.aspx
- DPAPI :
  http://msdn.microsoft.com/en-us/library/ms995355.aspx

2 - Vulnérabilité de la configuration par défaut du logiciel ElasticSearch

`ElasticSearch` est un logiciel de stockage et d'interrogation de données de type `NoSQL`. Il est souvent utilisé en conjonction avec `Logstash` et `Kibana`. Ce logiciel est conçu pour être déployé sur une ferme de serveurs, avec les différentes instances qui communiquent entre elles par divers moyens, dont aucun n'est authentifié. Un de ces modes de communication, actif par défaut, est une API `REST` au-dessus du protocole `HTTP`.

Les communications n'étant pas authentifiées, il est impératif de cloisonner les serveurs afin d'en interdire l'accès à des acteurs malveillants. Cependant, l'API `REST` présente une surface d'attaque supplémentaire : il est en effet possible de cibler un système inaccessible depuis Internet en utilisant un rebond via le navigateur web d'un utilisateur ou d'un développeur. Une requête de type `CSRF` peut permettre à un attaquant externe d'effectuer une action arbitraire sur un tel serveur.

Si un attaquant obtient (directement ou indirectement) un accès à la base de données, il aura dès lors tout loisir de lire, modifier, ou supprimer toutes les informations stockées dans la base. De plus, `ElasticSearch` offre une fonctionnalité dite « dynamic scripting », qui consiste en pratique à soumettre une classe Java arbitraire qui sera exécutée côté serveur, sans restriction (pas de « sandbox »). Cette fonctionnalité est maintenant désactivée dans la configuration par défaut à partir de la version 1.2.0, publiée le mois dernier.

De plus, un framework d'exploitation public intègre un code exploitant cette fonctionnalité et permettant de prendre le contrôle d'un serveur vulnérable.

Le CERT-FR recommande l'utilisation d'un sous-réseau dédié et isolé pour l'hébergement de la ferme `ElasticSearch`, ainsi que la désactivation du « dynamic scripting » en positionnant le paramètre `script.disable_dynamic: true` dans le fichier de configuration `elasticsearch.yml` sur chaque nœud. Il est également recommandé, si l'environnement le permet, de désactiver le mode de transport `REST` avec le paramètre `http.enabled: false`, ou à défaut de configurer le paramètre `http.cors.allow-origin` qui permet de limiter les sites autorisés à requêter le service depuis un navigateur Internet.

Documentation

- Configuration du mode de transport HTTP :
  http://www.elasticsearch.org/guide/en/elasticsearch/reference/current/modules-http.html
- http://bouk.co/blog/elasticsearch-rce/

3 - Mise à jour mensuelle Microsoft

Lors de sa dernière mise à jour mensuelle, Microsoft a publié six bulletins de sécurité, dont deux considérés comme critiques et trois comme importants :

- MS14-037 (critique) qui concerne Internet Explorer ;
- MS14-038 (critique) qui concerne le Journal de Windows ;
- MS14-039 (important) qui concerne le clavier visuel de Windows ;
- MS14-040 (important) qui concerne le pilote de gestion des sockets de Windows ;
- MS14-041 (important) qui concerne le composant DirectShow de Windows ;
- MS14-042 (modéré) qui concerne Microsoft Service Bus.

Ce mois-ci, Microsoft a corrigé de nombreuses vulnérabilités liées à des corruptions mémoire dans Internet Explorer susceptibles de conduire à l'exécution de code arbitraire à distance. Néanmoins aucune ne semble faire l'objet d'une exploitation active à ce jour et il n'y a pas de code d'exploitation public connu.

La vulnérabilité dans le clavier visuel de Windows pourrait permettre à un attaquant d'exécuter du code arbitraire au même niveau d'intégrité que l'utilisateur courant depuis un processus avec un faible niveau d'intégrité, par exemple une «sandbox» comme celle d'Internet Explorer (voir les articles au sujet des mécanismes de sandboxing dans les bulletins d'actualité précédents.)

La vulnérabilité dans le pilote de gestion des sockets de Windows pourrait permettre à un attaquant d'élever ses privilèges au niveau noyau.

Le CERT-FR recommande l'application de ces correctifs de sécurité dès que possible.

Le CERT-FR rappelle que Microsoft a cessé le support technique de Windows XP en avril 2014. Les bulletins de sécurité de Microsoft ne mentionnent donc plus explicitement ce système, mais cela ne signifie pas qu'il n'est pas vulnérable. De plus certaines tierces parties ont également cessé de fournir des mises à jour de sécurité pour Windows XP. C'est notamment le cas d'Oracle avec Java. En tout état de cause, le CERT-FR recommande de migrer rapidement vers des systèmes plus récents.

Documentation

- Bulletin de sécurité CERTFR-2014-AVI-300
  http://www.cert.ssi.gouv.fr/site/CERTFR-2014-AVI-300/index.html
- Bulletin de sécurité CERTFR-2014-AVI-301
  http://www.cert.ssi.gouv.fr/site/CERTFR-2014-AVI-301/index.html
- Bulletin de sécurité CERTFR-2014-AVI-302
  http://www.cert.ssi.gouv.fr/site/CERTFR-2014-AVI-302/index.html
- Bulletin de sécurité CERTFR-2014-AVI-303
  http://www.cert.ssi.gouv.fr/site/CERTFR-2014-AVI-303/index.html
- Bulletin de sécurité CERTFR-2014-AVI-304
  http://www.cert.ssi.gouv.fr/site/CERTFR-2014-AVI-304/index.html
- Bulletin de sécurité CERTFR-2014-AVI-305
  http://www.cert.ssi.gouv.fr/site/CERTFR-2014-AVI-305/index.html
- Bulletin d'actualité CERTFR-2014-ACT-025
  http://www.cert.ssi.gouv.fr/site/CERTFR-2014- ACT-025/index.html
- Bulletin d'actualité CERTFR-2014-ACT-026
  http://www.cert.ssi.gouv.fr/site/CERTFR-2014- ACT-026/index.html

4 - Rappel des avis émis

Dans la période du 04 au 10 juillet 2014, le CERT-FR a émis les publications suivantes :

- CERTFR-2014-AVI-296 : Multiples vulnérabilités dans PHP
- CERTFR-2014-AVI-297 : Multiples vulnérabilités dans Xen
- CERTFR-2014-AVI-298 : Vulnérabilité dans le noyau Linux d'Ubuntu
- CERTFR-2014-AVI-299 : Vulnérabilité dans les produits Huawei
- CERTFR-2014-AVI-300 : Multiples vulnérabilités dans Microsoft Internet Explorer
- CERTFR-2014-AVI-301 : Vulnérabilité dans Microsoft Windows

- CERTFR-2014-AVI-302 : Vulnérabilité dans Microsoft Windows
- CERTFR-2014-AVI-303 : Vulnérabilité dans Microsoft Windows
- CERTFR-2014-AVI-304 : Vulnérabilité dans Microsoft Windows
- CERTFR-2014-AVI-305 : Vulnérabilité dans Microsoft Service Bus
- CERTFR-2014-AVI-306 : Multiples vulnérabilités dans Adobe Flash Player
- CERTFR-2014-AVI-307 : Vulnérabilité dans les produits Cisco
- CERTFR-2014-AVI-308 : Multiples vulnérabilités dans Juniper Junos
- CERTFR-2014-AVI-309 : Multiples vulnérabilités dans les produits EMC

Gestion détaillée du document

11 juillet 2014 version initiale.