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 16 mai 2014
N° CERTFR-2014-ACT-020

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2014-ACT-020

1 - Les outils de vérification d'intégrité

La signature numérique d'un composant logiciel (programme exécutable, pilote noyau, bibliothèque, etc.) permet de vérifier l'authenticité du créateur du composant et l'intégrité du contenu. En particulier, ce mécanisme permet de garantir qu'un composant n'a pas été modifié depuis qu'il a été signé.

Vérifications automatiques par un système

Un système d'exploitation peut s'appuyer sur la signature numérique de programmes présents sur un système pour vérifier automatiquement leur intégrité. Le mécanisme de signature numérique conçu par Microsoft pour les systèmes Windows est appelé `Authenticode`. Basé sur des standards cryptographiques, ce mécanisme permet aux applications de modifier leur comportement au regard de la signature numérique identifiée (validité de la signature, confiance dans l'émetteur). Par exemple, la signature numérique fait partie des critères employés par Internet Explorer pour vérifier l'authenticité d'un programme et ainsi alerter l'utilisateur dans le cas d'une anomalie de signature.

De même, les boîtes de dialogue d'UAC (« User Account Control ») affichées lors de l'exécution d'un programme sont différentes si le programme est signé ou non. Une autre utilisation de la signature numérique concerne le chargement de pilote noyau : dans le cas de Windows XP, un avertissement est affiché lorsque l'utilisateur tente d'installer un pilote non signé. Pour les versions 64 bits de Windows et depuis Vista, le noyau exige que le pilote soit signé par une liste restreinte et identifiée d'autorités de certification pour le charger.

Linux n'utilise pas encore massivement de mécanisme de vérification de signatures de binaires, bien qu'un module ait été ajouté depuis la version 3.7 du noyau afin de gérer cette problématique et plus particulièrement la vérification de la signature d'un module noyau avant son chargement.

Vérifications de la signature numérique dans le cadre d'un incident de sécurité

Lors d'une analyse d'une compromission, la signature numérique est un bon moyen de vérifier automatiquement l'intégrité d'une grande quantité de composants logiciels. Sous Windows, le logiciel Process Explorer est capable de vérifier la signature de chaque exécutable en cours d'exécution, ainsi que les bibliothèques chargées par chaque processus. Il faut pour cela activer l'option *Verify Image Signatures* et ajouter l'affichage de la colonne *Verified Signer*. De manière analogue, le programme Autoruns permet de vérifier la signature de tous les binaires qui sont configurés en démarrage automatique, en activant l'option *Verify code signatures*. Ces deux logiciels font partie de la suite SysInternals.

Toutefois, le fonctionnement de ces outils peut être détourné par un code malveillant : il est ainsi recommandé de vérifier la signature des composants d'un système sur un système de confiance. Dans ce cas, d'autres outils peuvent être lancés depuis une machine d'analyse saine, sur des traces collectées sur un poste analysé. Les outils *SignTool* (de Microsoft) et *SigCheck* (de SysInternals) s'utilisent en ligne de commande et permettent la vérification d'un binaire passé en paramètre, que la signature soit embarquée ou qu'il soit signé via un catalogue de sécurité.

Les différentes distributions Linux utilisent peu la signature cryptographique de binaires et de paquets. Il existe cependant d'autres mécanismes de vérification d'intégrité de ces paquets qui diffèrent suivant les distributions. Par exemple, la distribution Debian a introduit "Secure APT" dans sa version 4.0 (Etch). Le fichier *Release.gpg* contenant une empreinte (« hash ») de chaque paquet `.deb` disponible sur un dépôt est généré, puis signé par la clé privée de l'archive Debian. La clé publique permettant de vérifier cette signature est préinstallée dans le répertoire `/etc/apt/trusted.gpg.d/`. L'installeur de paquet pourra vérifier que l'empreinte du fichier *Release.gpg* correspond effectivement à celle fournie dans la signature.

Il est possible de visualiser les clés publiques enregistrées grâce à la commande apt-key list pour vérifier qu'un attaquant n'a pas ajouté une clé non désirée. Le format `.deb` prévoit également un mécanisme pour signer un paquet directement, signature qui peut être vérifiée via l'outil *debsig-verify*, mais dans la pratique on constate que quasiment aucun paquet `.deb` n'est signé.

Dans le cas de Red Hat, on constate que les paquets RPM sont effectivement signés, et la signature peut être vérifiée à l'aide de la commande `rpm -K`.

Vérifications d'intégrité

Lorsque le mécanisme de signature cryptographique n'est pas disponible, l'analyste en investigation numérique peut s'appuyer sur les empreintes des fichiers.

Par exemple, sous Debian, l'outil debsums permet de vérifier rapidement l'intégrité des fichiers du système. Celui-ci s'appuie sur des fichiers d'extensions `.md5sums` présents dans la majorité des paquets Debian et qui contiennent les condensés de chaque fichier installé par le paquet. Ce fichier est conservé sur la machine après l'installation du paquet. On notera l'ajout récent de l'option `-verify` à la commande `dpkg` qui effectue les mêmes vérifications que debsums pour le moment, mais qui pourrait intégrer de nouvelles vérifications à l'avenir comme la modification des permissions d'un fichier.

Red Hat dispose déjà d'un outil de ce type. A chaque installation de paquet RPM, une base de données au format Berkeley est mise à jour avec les caractéristiques de chaque fichier installé par le paquet (condensé, permissions, date de modification, etc.). La commande `rpm -V` permet de vérifier à tout moment à l'aide de cette base de données que ces caractéristiques n'ont pas été altérées.

Bien sûr, étant donné que les fichiers `.md5sums` utilisés par `debsums` et la base de données utilisée par `rpm -V` sont stockés sur la machine analysée, ils peuvent tous deux être altérés par un attaquant.

Documentation

- Documentation SecureAPT Debian :
  https://wiki.debian.org/SecureApt
- Suite SysInternals :
  http://technet.microsoft.com/fr-FR/SysInternals

2 - Amélioration de la protection des secrets d'authentification sur les systèmes Windows (1/2)

Introduction

Sur les systèmes Windows 8.1, Microsoft a introduit de nouveaux mécanismes de sécurité.

Dédiées à la protection des secrets d'authentification, ces fonctionnalités visent à lutter contre l'extraction des condensats cryptographiques de mots de passe en mémoire. Ces mécanismes permettent de lutter contre la réalisation d'attaques de type « *pass-the-hash* » sans remédier au principe de l'attaque. Lors de la publication des correctifs de sécurité de mai 2014 Microsoft a décidé de rétroporter, *via* le KB 2871997, ces fonctionnalités de sécurité sur les systèmes Windows à partir de Windows 7 SP1.

Cet article est le premier d'une série de deux bulletins visant à décrire les mécanismes introduits par cette mise à jour et les gains en matière de sécurité.

Groupe de sécurité "protected users"

Un nouveau groupe de sécurité nommé « `protected users` » a été ajouté à l'annuaire Active Directory avec Windows Server 2012 R2. Les membres de ce groupe sont soumis à des restrictions non-configurables

des méthodes d'authentification qu'ils peuvent utiliser. Ainsi, les membres de ce groupe ne peuvent plus réaliser d'authentification utilisant NTLM, Digest ou CredSSP (utilisé notamment pour les connexions RDP). De plus, le système n'enregistre plus en mémoire les secrets permettant ce type d'authentification. Enfin, les contraintes de sécurité appliquées à Kerberos ont été durcies :

- la durée de vie du ticket de session (TGT) a été réduite à quatre heures ;
- seul l'algorithme AES est autorisé désactivant ainsi les algorithmes RC4 ou DES ;
- la délégation d'authentification Kerberos a été désactivée pour les membres de ce compte.

Cette fonctionnalité a été rétroportée par Microsoft pour l'ensemble des systèmes Windows à partir de Windows 7 SP1 afin de prendre en compte les restrictions devant être appliquées aux membres de ce groupe.

Implémentation du mode d'administration restreinte pour CredSSP

Intégré pour la première fois dans CredSSP sur Windows Server 2012 R2, le mode d'administration restreinte (« *Restricted Admin mode* ») est une fonctionnalité utilisée par le protocole RDP afin de limiter le risque de compromission des secrets d'authentification d'un client se connectant à distance sur un poste compromis. Si l'option « `restrictedAdmin` » est activée lors de la connexion du client au serveur *via* RDP, CredSSP se contente d'ouvrir une session utilisateur mais le système ne met pas en cache les secrets d'authentification de l'utilisateur.

Conclusion et recommandations

Annoncé depuis plusieurs mois, Microsoft propose, au travers des correctifs de mai 2014, un ensemble de solutions techniques permettant de lutter contre le vol de secrets cryptographiques fréquemment réalisé pour la mise en place d'attaques de type « *pass-the-hash* ». Améliorant la sécurité du système Windows, ces correctifs sont néanmoins susceptibles d'avoir des effets de bords sur certaines infrastructures. En effet, ces fonctionnalités modifiant le comportement des processus chargés de la validation des demandes d'authentification, elles sont susceptibles d'impacter le comportement des logiciels tiers s'interfaçant avec ces processus. Cependant, les gains en matière de sécurité sont indéniables et le CERT-FR recommande, après une phase de qualification approfondie, l'application de cette mise à jour.

Le prochain bulletin d'actualité décrira les autres améliorations apportés par cette mise à jour (restrictions de connexion des comptes locaux utilisateur, suppression de certains secrets d'authentification). Par la suite, d'autres bulletins détailleront la mise en œuvre de ces nouveaux mécanismes.

Documentation

- KB 2871997 :
  https://support.microsoft.com/kb/2871997

3 - Mise à jour mensuelle Microsoft

Lors de sa dernière mise à jour mensuelle, Microsoft a publié huit bulletins de sécurité, dont deux sont considérés critiques :

- MS14-022 (critique) qui concerne Microsoft SharePoint ;
- MS14-023 (important) qui concerne Microsoft Office ;
- MS14-024 (important) qui concerne un contrôle commun Microsoft (MSCOMCTL) ;
- MS14-025 (important) qui concerne les préférences de stratégie de groupe Microsoft ;
- MS14-026 (important) qui concerne Microsoft .NET Framework ;
- MS14-027 (important) qui concerne le gestionnaire de Shell Microsoft Windows ;
- MS14-028 (important) qui concerne Microsoft iSCSI ;
- MS14-029 (critique) qui concerne Microsoft Internet Explorer.

Microsoft a eu connaissance d'attaques exploitant les vulnérabilités :

- CVE-2014-1815 affectant Internet Explorer et corrigée dans le bulletin MS14-029 ;
- CVE-2014-1807 liée à l'association de fichiers dans le shell Windows et corrigée dans le bulletin MS14-027 ;
- CVE-2014-1812 au niveau des préférences de stratégie de groupe et corrigée dans le bulletin MS14-025 ;
- CVE-2014-1809 affectant un contrôle commun Microsoft et corrigée dans le bulletin MS14-024.

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

Documentation

- http://www.cert.ssi.gouv.fr/site/CERTFR-2014-AVI-220/index.html
- http://www.cert.ssi.gouv.fr/site/CERTFR-2014-AVI-221/index.html
- http://www.cert.ssi.gouv.fr/site/CERTFR-2014-AVI-222/index.html
- http://www.cert.ssi.gouv.fr/site/CERTFR-2014-AVI-223/index.html
- http://www.cert.ssi.gouv.fr/site/CERTFR-2014-AVI-224/index.html
- http://www.cert.ssi.gouv.fr/site/CERTFR-2014-AVI-225/index.html

4 - Rappel des avis émis

Dans la période du 09 au 15 mai 2014, le CERT-FR a émis les publications suivantes :

- CERTFR-2014-AVI-216 : Multiples vulnérabilités dans Cisco WebEx
- CERTFR-2014-AVI-217 : Vulnérabilité dans les produits Huawei
- CERTFR-2014-AVI-218 : Vulnérabilité dans le noyau Linux d'Ubuntu
- CERTFR-2014-AVI-219 : Multiples vulnérabilités dans le noyau Linux de Red Hat
- CERTFR-2014-AVI-220 : Multiples vulnérabilités dans Microsoft SharePoint
- CERTFR-2014-AVI-221 : Multiples vulnérabilités dans Microsoft Office
- CERTFR-2014-AVI-222 : Vulnérabilité dans un contrôle commun Microsoft
- CERTFR-2014-AVI-223 : Vulnérabilité dans les préférences de stratégie de groupe Microsoft
- CERTFR-2014-AVI-224 : Vulnérabilité dans Microsoft .NET Framework
- CERTFR-2014-AVI-225 : Vulnérabilité dans le gestionnaire de Shell Microsoft Windows
- CERTFR-2014-AVI-226 : Multiples vulnérabilités dans Microsoft iSCSI
- CERTFR-2014-AVI-227 : Multiples vulnérabilités dans Microsoft Internet Explorer
- CERTFR-2014-AVI-228 : Multiples vulnérabilités dans Adobe Flash Player
- CERTFR-2014-AVI-229 : Multiples vulnérabilités dans Adobe Reader et Acrobat
- CERTFR-2014-AVI-230 : Multiples vulnérabilités dans Google Chrome

Gestion détaillée du document

16 mai 2014 version initiale.