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 27 mars 2017
N° CERTFR-2017-ACT-013

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2017-ACT-013

1 - Publication d'une collision sur la fonction de hachage SHA-1.

La première réalisation pratique d'une attaque contre la fonction de hachage SHA-1 a été rendue publique le 23 février 2017 par Marc STEVENS et Pierre KARPMAN (*ENTRUM VOOR WISKUNDE EN INFORMATICA*, Amsterdam, Pays-Bas) et Elie BURSZTEIN, Ange ALBERTINI et Yarik MARKOV (*GOOGLE RESEARCH*).

Cette attaque permet de produire des *collisions* sur SHA-1, c'est-à-dire de trouver deux données ayant la même empreinte, avec un impact sur les applications de signature électronique. En effet, la première étape de la signature d'un document consiste à calculer son empreinte par une fonction de hachage.

Contexte historique

La possibilité théorique d'une telle attaque est admise dans le milieu académique depuis la publication de travaux de WANG, YIN et YU à Crypto 2005. Ces travaux ont été progressivement améliorés ; la technique de cryptanalyse aujourd'hui considérée comme la plus efficace ayant été publiée par STEVENS à Eurocrypt 2013.

Depuis cette date, les résultats les plus marquants concernent des exploitations pratiques de cette attaque, qui ont nécessité des efforts conséquents d'implémentation sur processeur graphique et une grande puissance de calcul ; mais dont l'issue était quasi-certaine. En 2015, STEVENS, KARPMAN et PEYRIN ont publié la première collision sur la seule fonction de compression de SHA-1 qui n'avait pas d'impact pratique direct.

Cependant, la puissance de calcul nécessaire à sa réalisation est proche de celle qui permet de trouver des collisions complètes, ce qui a été finalement réalisé en 2017.

Adaptation au format pdf

Les attaques en recherche de collisions contre des fonctions de hachage qui font l'objet de publications académiques permettent généralement de trouver des collisions dites *non significatives*, en ce sens qu'elles permettent de trouver deux messages ayant la même empreinte mais sans que l'attaquant ne puisse choisir la signification de ces messages, ni même garantir qu'ils respectent un format de fichier donné.

Une telle restriction pourrait paraître importante au premier abord : en effet, en appliquant directement une telle technique, un attaquant pourrait obtenir une collision, mais n'aurait quasiment aucune chance de pouvoir l'exploiter. Toutefois, il est communément admis par les experts qu'une telle difficulté est relativement facile à contourner. Par exemple, dès 2005, DAUM et LUCKS montrent qu'il est très facile d'adapter une attaque contre la fonction MD5 pour produire deux documents au format PostScript ayant la même empreinte, dont ils ont pu intégralement choisir le contenu. L'attaque contre SHA-1 publiée le 21 février utilise une technique similaire pour s'adapter au format pdf.

Position de l'ANSSI

Pour les raisons évoquées ci-dessus, la découverte effective d'une collision pour SHA-1 était prévisible et avait depuis longtemps été anticipée par l'ANSSI. Le Référentiel Général de Sécurité mentionne explicitement SHA-1

comme non conforme aux règles qu'il impose, et ce depuis sa publication en 2010. Les versions antérieures du référentiel des mécanismes cryptographiques de l'ANSSI apportaient cette même précision depuis la mise à jour de 2007.

L'utilisation de mécanismes cryptographiques de signature reposant sur SHA-1 est à présent l'objet d'une vulnérabilité immédiatement exploitable et doit être abandonnée. Pour d'autres applications (dérivation de clés, génération de nombres aléatoires, authentification de messages), même si cette vulnérabilité est moins directement exploitable, il est fortement recommandé de privilégier l'utilisation d'une fonction de hachage à l'état de l'art, comme SHA-2 ou SHA-3.

Documentation

The first collision for full SHA-1, M. STEVENS, E. BURZSTEIN, P. KARPMAN, A. ALBERTINI et Y. MARKOV
http://shattered.io/static/shattered.pdf

2 - Rançongiciel HakunaMatata

Le CERT-FR a constaté depuis plusieurs semaines une augmentation significative du nombre d'incidents de sécurité impliquant le rançongiciel nommé HakunaMatata. Le fonctionnement du code est classique pour un code malveillant de cette famille : il procède au chiffrement des fichiers, ajoute l'extension ".hakunamatata" puis affiche la demande de rançon.

L'originalité de ce code malveillant concerne sa méthode de propagation. Les incidents rencontrés par le CERT-FR appuient l'hypothèse d'une infection initiale basée sur le service RDP accessible depuis Internet. Un mot de passe faible ou dérobé est à l'origine de l'ouverture de session à distance.

Recommandations

Si les bonnes pratiques afin de se prémunir contre les rançongiciels sont toujours applicables, ce mode opératoire rappelle également la nécessité de protéger les accès aux services d'administration à distance. Dans ce cas précis, le risque de compromission du fait de l'exposition du service RDP à Internet doit être évalué : ce service ne doit être accessible sur Internet si cela est strictement nécessaire. Dans tous les cas, une politique de mot de passe adaptée doit être appliquée afin d'éviter un accès opportuniste à un service d'administrations à distance (attaque par force brute, mot de passe trivial, etc.).

Par ailleurs, un audit régulier de la surface d'exposition d'un système d'information à Internet permet de détecter au plus tôt un défaut de configuration d'un équipement réseau ou une régression des règles de filtrage.

3 - Rappel des avis émis

Dans la période du 20 au 26 mars 2017, le CERT-FR a émis les publications suivantes :

- CERTFR-2017-ALE-005 : Vulnérabilité dans les commutateurs Cisco
- CERTFR-2017-AVI-087 : Multiples vulnérabilités dans Moodle
- CERTFR-2017-AVI-088 : Vulnérabilité dans Mozilla Firefox
- CERTFR-2017-AVI-089 : Multiples vulnérabilités dans les produits Cisco
- CERTFR-2017-AVI-090 : Multiples vulnérabilités dans NTP
- CERTFR-2017-AVI-091 : Vulnérabilité dans Samba

Gestion détaillée du document

27 mars 2017 version initiale.