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 19 octobre 2015
N° CERTFR-2015-ACT-042

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2015-ACT-042

1 - Ouverture du compte Twitter de l'ANSSI

Le 12 octobre 2015, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) a ouvert le compte Twitter @ANSSI_FR afin d'informer un large public sur ses activités et actualités. Ce compte sera notamment utilisé pour relayer les publications de l'ANSSI, et en particulier les guides techniques disponibles sur le site Internet de l'Agence.

A noter que le CERT-FR n'est, pour le moment, pas présent sur le réseau de micro-blogging Twitter.

2 - What's SHAppening?

Rappel cryptographique

Une fonction de hachage cryptographique prend en entrée un message de taille arbitraire et produit un condensat de taille fixe. Une bonne fonction de hachage H est conçue pour être résistante aux collisions : un attaquant ne doit pas pouvoir facilement trouver deux messages différents M1 et M2 dont le condensat serait identique : `H(M1) = H(M2)`. La construction algorithmique Merkle-Damgård est utilisée pour répondre à ce problème et repose sur l'utilisation itérative d'une fonction de compression. Le message est découpé en blocs de taille fixe, chacun de ces blocs est ensuite traité par la fonction de compression puis le résultat est transmis au bloc suivant. Si cette dernière est résistante aux collisions, alors la fonction de hachage l'est aussi.

SHA-1

De nombreux protocoles et applications centraux au fonctionnement d'Internet tels que TLS/SSL, PGP, SSH, S/MIME ou IPsec font usage de condensats dans les mécanismes de vérification d'intégrité, d'authentification ou de génération de signatures électroniques. Ce système permet de sécuriser les transactions bancaires, le stockage des mots de passe ou encore la distribution de logiciels. Parmi les fonctions de hachage les plus répandues aujourd'hui, on trouve entre autres MD5 et SHA-1.

SHA-1 est une fonction publiée par le NIST, dont la première version date de 1995. Un certain nombre d'attaques, bien que théoriques, publiées depuis 2005 prouvent que SHA-1 est cassée. Ainsi, le NIST déconseille l'utilisation de SHA-1 depuis mars 2006 [1] et une décision du CA/B Forum du 16 octobre 2014 préconise le retrait de SHA-1 d'ici fin 2016 (voir bulletin d'actualité CERTFR-2015-ACT-018 du 4 mai 2015 [2]).

Cette date de retrait de SHA-1 pourrait être remise en cause par la publication récente d'une attaque baptisée "*The SHAppening*" [3]. L'équipe de chercheurs, composée de Marc Stevens, Pierre Karpman et Thomas Peyrin, a réussi à trouver des collisions dans la fonction de compression interne. Or la fiabilité d'une fonction de hachage repose sur celle de la fonction de compression interne : s'il est possible d'y trouver une collision, alors elle ne doit plus être utilisée et elle doit être considérée comme cassée. C'est la première attaque pratique à démontrer la faiblesse de SHA-1. Les précédentes attaques, bien que théoriquement valides, étaient estimées trop coûteuses pour être mises en oeuvre. Bruce Schneier estimait en 2012 [4] que le coût d'une attaque par collision serait de

700 000 dollars en 2015. Aujourd'hui, les chercheurs estiment qu'en utilisant des GPU, l'attaque serait réalisable avec un budget estimé entre 75 000 et 120 000 dollars, ce qui serait à la portée de groupes d'attaquants ou de gouvernements.

Conséquences

MD5, autrefois fonction de hachage la plus répandue, a continué à être utilisée quand bien même son obsolescence était avérée. Les conséquences furent importantes : le système entier des autorités de certification, sur lequel sont basés de nombreux protocoles et mécanismes de sécurité, s'est retrouvé menacé par une attaque aboutissant à la création d'une autorité de certification intermédiaire indésirable [5]. Actuellement, les condensats SHA-1 sont encore utilisés dans la signature numérique d'environ 30% des certificats. Afin d'éviter des incidents similaires à ceux survenus avec l'utilisation de MD5, il est recommandé de ne pas attendre le retrait officiel de SHA-1 fin 2016 pour migrer vers SHA-2 ou SHA-3.

Enfin, il est important de rappeler que l'annexe B1 du référentiel général de sécurité (RGS v2.0) mentionne, à la section 2.3, que le mécanisme de hachage SHA-1 ne lui est pas conforme [6].

Références

1. NIST's March 2006 Policy on Hash Functions (15 mars 2006)
   http://csrc.nist.gov/groups/ST/hash/policy_2006.html
2. Bulletin d'actualité CERTFR-2015-ACT-018 (4 mai 2015)
   http://www.cert.ssi.gouv.fr/site/CERTFR-2015-ACT-018.pdf
3. The SHAppening: freestart collisions for SHA-1 (8 octobre 2015)
   https://sites.google.com/site/itstheshappening/
4. When Will We See Collisions for SHA-1? (5 octobre 2012)
   https://www.schneier.com/blog/archives/2012/10/when_will_we_se.html
5. MD5 considered harmful today - Creating a rogue CA certificate (30 décembre 2008)
   http://www.win.tue.nl/hashclash/rogue-ca/
6. Annexe B1 sur les mécanismes cryptographiques du référentiel général de sécurité 2.0 (version 2.03 du 21 février 2014)
   http://www.ssi.gouv.fr/uploads/2014/11/RGS_v-2-0_B1.pdf

3 - Mise à jour mensuelle de Microsoft

Le 13 octobre 2015, Microsoft a publié six bulletins de sécurité, dont trois sont considérés comme critiques et trois comme importants :

- MS15-106 (critique) qui concerne Internet Explorer ;
- MS15-107 (important) qui concerne Microsoft Edge ;
- MS15-108 (critique) qui concerne les moteurs d'exécution VBScript et JScript ;
- MS15-109 (critique) qui concerne Windows Shell ;
- MS15-110 (important) qui concerne Microsoft Office ;
- MS15-111 (important) qui concerne le noyau de Windows.

Les navigateurs de Microsoft, Internet Explorer et Edge, font l'objet de bulletins. La mise à jour d'Internet Explorer (bulletin MS15-106) corrige quatorze vulnérabilités qui peuvent notamment conduire à une exécution de code à distance, une élévation de privilège, une fuite d'information ou à un contournement de mécanismes de sécurité tels que la disposition aléatoire de l'espace d'adressage. Concernant Microsoft Edge (bulletin MS15-107), deux vulnérabilités sont corrigées ; l'une d'entres-elles permet notamment de contourner le filtre de protection contre les scripts inter-sites (XSS). Pour les deux navigateurs, l'exploitation de ces vulnérabilités nécessite qu'un utilisateur visite une page spécialement conçue.

Les moteurs d'exécution VBScript et JScript sont touchés par deux vulnérabilités (bulletin MS15-108). Elles peuvent conduire à une exécution de code arbitraire à distance si un utilisateur consulte une page Web malveillante ou ouvre un document dans Microsoft Office faisant appel au moteur de rendu d'Internet Explorer. On peut aussi noter que ces deux vulnérabilités font aussi partie des quinze corrigées dans Internet Explorer.

Le bulletin MS15-109 corrige quant à lui deux vulnérabilités dans Windows Shell. Ces deux vulnérabilités concernent la gestion en mémoire de certains objets liés à l'interface graphique. Elles peuvent conduire à une exécution de code arbitraire à distance. L'une de ces deux vulnérabilités est exploitable par l'intermédiaire d'Internet Explorer.

Microsoft Office fait l'objet de la correction de six vulnérabilités (bulletin MS15-110) pouvant conduire à une exécution de code arbitraire à distance ; elles portent principalement sur la gestion des données en mémoire liée à l'ouverture de documents. Concernant Microsoft SharePoint Server, la vulnérabilité concerne une mauvaise gestion des fichiers de définition de types de document (DTD), permettant ainsi d'accéder au contenu de fichiers arbitraires sur le serveur. Enfin, Microsoft Office Web Apps se voit corrigé d'une vulnérabilité permettant de contourner les filtres contre les scripts inter-sites.

Enfin, cinq vulnérabilités sont corrigées au niveau du noyau de Windows (bulletin MS15-111). Plusieurs d'entres-elles peuvent conduire à une élévation de privilège permettant ainsi à un attaquant d'exécuter du code en mode noyau. Une vulnérabilité permettant de contourner la fonctionnalité de démarrage sécurisé Trusted Boot est aussi corrigée : elle permet d'injecter des paramètres malveillants dans les données de configuration de démarrage (BCD). Son exploitation permet de contourner les tests d'intégrité réalisés au démarrage et ainsi d'exécuter du code non signé.

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

Documentation

- Bulletin de sécurité Microsoft MS15-106
  https://technet.microsoft.com/library/security/MS15-106
- Bulletin de sécurité Microsoft MS15-107
  https://technet.microsoft.com/library/security/MS15-107
- Bulletin de sécurité Microsoft MS15-108
  https://technet.microsoft.com/library/security/MS15-108
- Bulletin de sécurité Microsoft MS15-109
  https://technet.microsoft.com/library/security/MS15-109
- Bulletin de sécurité Microsoft MS15-110
  https://technet.microsoft.com/library/security/MS15-110
- Bulletin de sécurité Microsoft MS15-111
  https://technet.microsoft.com/library/security/MS15-111
- Avis de sécurité CERTFR-2015-AVI-421
  http://cert.ssi.gouv.fr/site/CERTFR-2015-AVI-421
- Avis de sécurité CERTFR-2015-AVI-422
  http://cert.ssi.gouv.fr/site/CERTFR-2015-AVI-422
- Avis de sécurité CERTFR-2015-AVI-423
  http://cert.ssi.gouv.fr/site/CERTFR-2015-AVI-423
- Avis de sécurité CERTFR-2015-AVI-424
  http://cert.ssi.gouv.fr/site/CERTFR-2015-AVI-424
- Avis de sécurité CERTFR-2015-AVI-425
  http://cert.ssi.gouv.fr/site/CERTFR-2015-AVI-425
- Avis de sécurité CERTFR-2015-AVI-426
  http://cert.ssi.gouv.fr/site/CERTFR-2015-AVI-426

4 - Rappel des avis émis

Dans la période du 12 au 18 octobre 2015, le CERT-FR a émis les publications suivantes :

- CERTFR-2015-ALE-011 : Vulnérabilité dans Adobe Flash Player
- CERTFR-2015-AVI-421 : Multiples vulnérabilités dans Microsoft Internet Explorer
- CERTFR-2015-AVI-422 : Multiples vulnérabilités dans Microsoft Edge
- CERTFR-2015-AVI-423 : Multiples vulnérabilités dans VBScript et Jscript de Microsoft Windows
- CERTFR-2015-AVI-424 : Multiples vulnérabilités dans Microsoft Windows Shell
- CERTFR-2015-AVI-425 : Multiples vulnérabilités dans Microsoft Office

- CERTFR-2015-AVI-426 : Multiples vulnérabilités dans le noyau de Microsoft Windows
- CERTFR-2015-AVI-427 : Multiples vulnérabilités dans Adobe Acrobat Reader
- CERTFR-2015-AVI-428 : Multiples vulnérabilités dans Adobe Flash Player
- CERTFR-2015-AVI-429 : Multiples vulnérabilités dans Google Chrome
- CERTFR-2015-AVI-430 : Multiples vulnérabilités dans le noyau Linux de Debian
- CERTFR-2015-AVI-431 : Multiples vulnérabilités dans les produits Juniper
- CERTFR-2015-AVI-432 : Vulnérabilité dans Mozilla Firefox

Gestion détaillée du document

19 octobre 2015 version initiale.