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 05 octobre 2015
N° CERTFR-2015-ACT-040

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2015-ACT-040

1 - Nouvelles protections Flash

Depuis le début de l'année 2015, Adobe fait face à une recrudescence des vulnérabilités impactant son logiciel Flash Player. Afin d'endiguer ce phénomène, de nouvelles stratégies ont été mises en place dans la version 18.0.0.209 de Flash publiée le 14 juillet 2015, afin de complexifier l'exploitation de nouvelles vulnérabilités. Ces dispositifs ont été développés via une collaboration entre Adobe et l'équipe Project Zero de Google.

La plupart des dernières vulnérabilités Flash ont été exploitées en écrasant la taille d'un objet vecteur. En effet, cette technique permet de contourner la disposition stochastique de l'espace mémoire (ASLR) et la protection NX/DEP. Pour être en mesure d'écraser un objet vecteur, l'attaquant va d'abord réaliser un massage du tas de manière à pouvoir déterminer l'emplacement de l'objet ciblé.

Plusieurs stratégies sont mises en place pour empêcher la corruption de cet objet. Tout d'abord, les objets vecteurs sont placés sur un tas différent des autres objets Flash. Cette fonctionnalité a d'abord été implémentée uniquement sous Chrome puis sur les autres navigateurs depuis la version 18.0.0.232 de Flash Player. La disposition stochastique de l'espace mémoire (ASLR) a également été renforcée. Auparavant, il était possible de prédire plus ou moins précisément l'emplacement d'un objet en mémoire comme les structures PEB et TEB. Enfin, l'intégrité du champ représentant la taille de l'objet vecteur est préservée en lui associant un secret qui sera vérifié via une opération "ou-exclusif". Si lors de l'utilisation de l'objet la valeur n'est pas correctement vérifiée, une erreur est levée et le programme est terminé.

Ces stratégies ne sont malheureusement pas sans défaut comme le prouvent trois méthodes présentées récemment par l'équipe Project Zero permettant de contourner les protections mises en place. Un attaquant peut aisément contourner la protection apportée à la taille de l'objet vecteur en devinant ou en retrouvant le secret en mémoire. Ainsi les trois contournements présentés par Project Zero ciblent l'emplacement du secret situé dans l'entête de l'objet vecteur. Trois champs dans l'entête sont importants : le champ taille, le résultat du "ou-exclusif" entre la taille et le secret puis un pointeur vers le secret en lui-même. Ainsi un attaquant pourrait forger un entête via une vulnérabilité de type dépassement de tampon de manière à rediriger le pointeur vers une valeur contrôlée, cette valeur devant satisfaire l'opération "ou-exclusif".

Le premier exemple est cependant théorique et uniquement valable sur les systèmes 32bits. En effet, ce contournement nécessite d'allouer une très grande quantité de données ne contenant que des zéros puis d'y rediriger le pointeur. Le secret devient donc 0. L'attaquant peut ensuite forger l'entête de l'objet vecteur en spécifiant la taille désirée puis en plaçant cette même taille dans le champ correspondant au résultat du "ou-exclusif" puisque l'opération sera effectuée sur zéro.

Le deuxième contournement exploite la présence d'une zone mémoire particulière existant sous les systèmes d'exploitation Windows, appelée User Shared Data. Cette zone mémoire située à une adresse fixe est connue pour être utilisée lors de contournement de la disposition stochastique de l'espace mémoire (ASLR). Le début cette plage mémoire est remplie de zéro. Il suffit donc à l'attaquant de modifier le pointeur indiquant le secret vers cet emplacement. Comme pour le contournement précédent, le résultat du "ou-exclusif" devient la taille du vecteur.

Linux n'est pas en reste face à cette technique. En effet, la zone mémoire vsyscall peut être utilisée de manière similaire. Située à une adresse fixe, elle ne contient pas de zéro mais une valeur fixe 0xccccccccc. Cette zone

mémoire est désactivée sur les systèmes Linux modernes.

Le dernier contournement présenté par Project Zero est valable si la zone mémoire vsyscall est désactivée, et se base sur la réécriture partielle du pointeur indiquant le secret. Juste après le secret, la structure vecteur n'est composée que de zéro. L'objectif est donc de dévier le pointeur de manière à le rediriger juste après l'emplacement où est stocké le secret. Pour cela, le dépassement de tampon utilisé doit être suffisamment précis pour n'écraser que la partie faible de l'octet du pointeur. Le pointeur doit également être aligné en mémoire.

Ces contournements ont été corrigés au sein de la version 18.0.0.232 de Flash Player. Ainsi un jeu du chat et de la souris débute entre les ingénieurs en sécurité impliqués dans la protection et l'analyse de vulnérabilités Flash et les attaquants. Lorsque le temps nécessaire à l'exploitation d'une vulnérabilité Flash excédera son profit, les attaquants déplaceront probablement leurs efforts vers un nouveau vecteur d'attaque.

Malgré l'amélioration significative de la sécurité du logiciel Flash Player, Le CERT-FR recommande aux utilisateurs de rester vigilants et d'appliquer assidûment les correctifs disponibles.

Documentations

- https://helpx.adobe.com/security/products/flash-player/apsb15-18.html
- http://googleprojectzero.blogspot.fr/2015/07/significant-flash-exploit-mitigations_16.html
- http://googleprojectzero.blogspot.fr/2015/08/three-bypasses-and-fix-for-one-of.html

2 - Rappel des avis émis

Dans la période du 28 septembre au 04 octobre 2015, le CERT-FR a émis les publications suivantes :

- CERTFR-2015-AVI-410 : Vulnérabilité dans le pilote graphique NVIDIA
- CERTFR-2015-AVI-411 : Multiples vulnérabilités dans le noyau Linux Ubuntu
- CERTFR-2015-AVI-412 : Multiples vulnérabilités dans les produits Huawei
- CERTFR-2015-AVI-413 : Multiples vulnérabilités dans les produits VMWare
- CERTFR-2015-AVI-414 : Multiples vulnérabilités dans Apple Safari
- CERTFR-2015-AVI-415 : Vulnérabilité dans Apple iOS
- CERTFR-2015-AVI-416 : Multiples vulnérabilités dans Apple OS X

Gestion détaillée du document

05 octobre 2015 version initiale.