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 février 2017
N° CERTFR-2017-ACT-009

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2017-ACT-009

1 - Protection DesktopVerifyHeapUnicodeString

La mise à jour anniversaire de Windows 10 (14393) comporte de nouvelles contre-mesures. Notamment, une mise à jour vise à renforcer la sécurité du système d'exploitation à l'encontre d'exploits liés au composant win32k. Ce composant, présent depuis les premières versions de Windows, a évolué à maintes reprises (migré du monde utilisateur vers le monde noyau) et est une cible de choix pour les attaquants.

Lors de l'exploitation de vulnérabilités impactant le noyau, l'attaquant cherche à obtenir des primitives de lecture et écriture dans le but d'exécuter sa charge utile avec des privilèges élevés. Pour ce faire, une technique publique et utilisée par certains groupes d'attaquants consiste en la corruption de l'objet strName de type LARGE_UNICODE_STRING. Cet objet intégré à un objet Window (tagWND) correspond au titre de la fenêtre.

La modification de l'adresse de base l'objet strName couplé à l'utilisation des fonctions InternalGetWindowText et NtUserDefSetText permettent de respectivement lire et écrire des données en zone noyau.

La contre-mesure, implémentée au sein de la fonction DesktopVerifyHeapUnicodeString a été intégrée à ces deux fonctions. Cette fonction vérifie les propriétés de la structure LARGE_UNICODE_STRING (length, MaximumLength et buffer) qui sera manipulée par la fonction. Certains de ces contrôles s'appuient sur les caractéristiques de la zone mémoire allouée pour les objets graphiques associés au bureau courant (tagDESKTOP).

Cette contre-mesure réduit les possibilités de lecture et écriture de l'attaquant à la zone mémoire alloué pour les objets graphiques du bureau courant.

Cependant, une technique d'exploitation présentée lors de la conférence BlackHat Europe 2016 permettrait de contourner cette contre-mesure. Celle-ci repose sur la corruption du champ cbwnExtra et l'utilisation du tableau WindowExtraData de l'objet Window. En couplant la corruption de ce champ aux fonctions GetWindowLongW et SetWindowLongW, il est possible d'obtenir une première primitive de lecture et écriture. En juxtaposant deux objets Window, cette première primitive permettrait de corrompre le deuxième objet Window. L'objet correspondant au bureau courant utilisé par la contre-mesure est intégré à la structure Window. La technique consiste en la corruption de l'objet strName et de l'objet tagDESKTOP afin de valider l'ensemble des contrôles de sécurité.

Malgré les limitations de cette contre-mesure, le noyau Windows se voit ainsi doté d'une nouvelle protection augmentant la difficulté de son exploitation. Elle s'inscrit dans la stratégie de Microsoft qui consiste, entre autres, à casser les techniques d'exploitation connues.

Documentation

- https://blogs.technet.microsoft.com/mmpc/2017/01/13/hardening-windows-10-with-zero-day-exploit-mitigations/
- https://www.virusbulletin.com/uploads/pdf/conference_slides/2015/OhFlorio-VB2015.pdf
- https://www.blackhat.com/docs/eu-16/materials/eu-16-Liang-Attacking-Windows-By-Windows.pdf
- https://improsec.com/blog//hardening-windows-10-with-zero-day-exploit-mitigations-under-the-microscope

2 - Rappel des avis émis

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

- CERTFR-2017-ALE-002 : Vulnérabilité dans Microsoft Windows
- CERTFR-2017-AVI-054 : Multiples vulnérabilités dans le noyau Linux de Suse
- CERTFR-2017-AVI-055 : Multiples vulnérabilités dans Adobe Flash Player sur Windows
- CERTFR-2017-AVI-056 : Vulnérabilité dans Xen
- CERTFR-2017-AVI-057 : Multiples vulnérabilités dans Citrix XenServer
- CERTFR-2017-AVI-058 : Multiples vulnérabilités dans le noyau Linux d'Ubuntu
- CERTFR-2017-AVI-059 : Multiples vulnérabilités dans SCADA Siemens RUGGEDCOM NMS

Gestion détaillée du document

27 février 2017 version initiale.