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 06 février 2017
N° CERTFR-2017-ACT-006

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2017-ACT-006

1 - Protection RFG (Return Flow Guard) de Windows 10

La version RS2 de Windows 10 propose une nouvelle contre-mesure nommée RFG (Return Flow Guard). Il s'agit de protéger les applications d'une catégorie d'attaques utilisant la pile pour contrôler le déroulement de leur exécution.

Les programmes optant pour RFG se voient dotés d'une pile fantôme annexe (la "shadow stack") où les adresses de retours des fonctions sont dupliquées. Pour un attaquant, l'usurpation d'une adresse de retour corrompue afin de détourner le flot de contrôle de l'application, ou la technique de ROP (Return Oriented Programming) devient beaucoup plus difficile à mettre en oeuvre du fait de cette pile fantôme.

RFG repose sur la collaboration du compilateur et du chargeur d'exécutable. Le compilateur insère au prologue et à l'épilogue de chaque fonction quelques instructions inertes qui tiennent simplement lieu de tampon.

Lors du chargement, et si le système d'exploitation offre la protection RFG, ces tampons sont remplis par deux petites séquences d'instructions utiles dont le rôle est de copier l'adresse de retour sur la pile fantôme, lors du prologue, puis de vérifier que celle-ci n'a pas été corrompue en la comparant à sa copie, lors de l'épilogue des fonctions.

Pour accéder à la pile fantôme rapidement, Windows 10 mobilise le registre de segment FS (inutilisé en 64-bit jusqu'ici) pour y stocker l'adresse de base de la pile. Dès lors, les accès mémoire préfixés par FS lisent ou écrivent le contenu de la pile fantôme. L'adresse de retour d'une fonction, pointée par le registre RSP à l'entrée dans la fonction, est dupliquée à l'offset RSP du segment FS dans la pile fantôme. Les deux piles croissent et décroissent donc parallèlement. Le pointeur de pile RSP sert d'index dans les deux piles.

Un désavantage possible de cette technique est l'usage mémoire: de fait, la taille de pile est doublée. La pile fantôme, en dépit du fait qu'elle ne contient que les copies des adresses de retour mais aucun paramètre ou variable locale, utilise autant de pages mémoire que la pile principale. Les adresses de retour y apparaissent très espacées. Tel n'est pas le cas de la future technologie CET (Control-Flow Enforcement Technology) d'Intel (cf bulletin d'actualité CERTFR-2016-ACT-027), où la pile fantôme proposée est plus compacte car les copies d'adresses de retour y sont contigues et que celle-là possède son propre pointeur de pile.

L'implantation matérielle permet à Intel de proposer une solution plus aboutie, mais le RFG de Microsoft, s'il n'a pas le luxe d'un fondement matériel, offre l'avantage de s'adapter à la plupart des processeurs existants. Parmi les différences entre CET et RFG, on peut également mentionner la protection en écriture de la pile fantôme de CET, alors qu'elle doit être autorisée en écriture pour RFG. On peut supposer que les attaquants essaieront d'exploiter cette faiblesse.

Il est aussi possible de comparer RFG à la contre-mesure RAP proposée par PaX Team (cf CERTFR-2015-ACT-047). Comme RFG, la protection RAP est purement logicielle. RAP ne repose pas sur une pile fantôme séparée de la pile principale. Les adresses de retour sont copiées dans un registre témoin protégé par un masque aléatoire. Dans le cas de RFG comme de RAP, si la conception générale est solide, on ne peut exclure des voies d'attaques reposant sur le cadre concret de telle ou telle application: un programme pourrait offrir un gadget susceptible de modifier la valeur de FS avant de déclencher une chaîne ROP (pour RFG) ou de deviner la valeur du masque aléatoire (pour RAP).

RFG poursuit donc l'amélioration de la sécurité des systèmes Windows, et comble un manque du mécanisme CFG (Control-Flow Guard) déjà existant en protégeant les adresses de retours sur la pile. La multiplication de tels mécanismes offre une couverture croissante des voies d'exploitation des corruptions mémoire, même si le problème fondamental de l'existence de ces corruptions demeure.

2 - Rappel des avis émis

Dans la période du 30 janvier au 05 février 2017, le CERT-FR a émis les publications suivantes :

- CERTFR-2017-AVI-034 : Multiples vulnérabilités dans le noyau Linux de SUSE
- CERTFR-2017-AVI-035 : Multiples vulnérabilités dans les produits Cisco
- CERTFR-2017-AVI-036 : Vulnérabilité dans Cisco WebEx Browser Extension
- CERTFR-2017-AVI-037 : Multiples vulnérabilités dans VMware Airwatch
- CERTFR-2017-AVI-038 : Vulnérabilité dans Cisco Prime Home
- CERTFR-2017-AVI-039 : Multiples vulnérabilités dans le noyau Linux d'Ubuntu

Durant la même période, les publications suivantes ont été mises à jour :

- CERTFR-2017-ALE-001 : Vulnérabilité dans Cisco WebEx (clôture de l'alerte.)

Gestion détaillée du document

06 février 2017 version initiale.