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 04 juillet 2016
N° CERTFR-2016-ACT-027

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2016-ACT-027

1 - Intel annonce les spécifications d'une nouvelle technologie de protection

Le 9 juin 2016, Intel a publié les spécifications d'une nouvelle technologie permettant de rendre plus difficile l'exploitation de certaines vulnérabilités. Ce mécanisme, nommé « Control-flow Enforcement Technology » (CET), est géré directement au niveau du processeur. Il est garant de l'intégrité du flot de contrôle lors de l'exécution d'un programme.

Fonctionnement technique

Lors de l'exécution d'un programme, une région mémoire appelée « la pile » permet de stocker des données (arguments des fonctions, variables locales, etc.) et des informations concernant le transfert du flot de contrôle (adresses de retour de fonctions). Intel CET définit une seconde pile, nommée « pile fantôme », qui est utilisée exclusivement lors des opérations de transfert du flot de contrôle. La pile fantôme se situe dans une région mémoire spéciale, protégée contre l'écriture grâce à des modifications dans la table des pages. Ces modifications permettent de s'assurer de son intégrité et d'empêcher sa corruption ou sa modification.

Seulement 2 instructions permettent de manipuler la pile fantôme :

- `CALL` : empile l'adresse de retour de la fonction sur la pile fantôme (en plus de le faire sur la pile traditionnelle) ;
- `RET` : dépile l'adresse de retour de la pile fantôme et la compare avec celle de la pile traditionnelle.

Après une instruction `RET`, le programme continue de s'exécuter uniquement si les adresses correspondent. En effet, si les adresses récupérées par l'instruction `RET` sont différentes, alors une corruption mémoire, due probablement à une tentative d'exploitation de vulnérabilité, a eu lieu. Dans ce cas, le programme stoppe son exécution.

De plus, l'instruction `ENDBRANCH` a été ajoutée au jeu d'instructions. Elle permet de marquer une adresse comme étant la destination possible d'un saut indirect (utilisé par exemple, dans le cas de la directive "switch" en C). Ainsi, lors de l'exécution d'un programme, si un saut dynamique n'a pas pour destination une instruction `ENDBRANCH`, le processeur génère une exception. Ce mécanisme vise à empêcher certaines techniques d'exploitation, comme ROP.

La documentation complète du fonctionnement de CET est disponible ci-dessous.

Documentation

- Article du blog Intel :
  https://blogs.intel.com/evangelists/2016/06/09/intel-release-new-technology-specifications-protect-rop-attacks/
- Documentation complète :
  https://software.intel.com/sites/default/files/managed/4d/2a/control-flow-enforcement-technology-preview.pdf

2 - Rappel des avis émis

Dans la période du 27 juin au 03 juillet 2016, le CERT-FR a émis les publications suivantes :

- CERTFR-2016-AVI-219 : Vulnérabilité dans Blue Coat PacketShaper S-Series
- CERTFR-2016-AVI-220 : Multiples vulnérabilités dans le noyau Linux d'Ubuntu
- CERTFR-2016-AVI-221 : Vulnérabilité dans LibreOffice
- CERTFR-2016-AVI-222 : Multiples vulnérabilités dans les produits Symantec
- CERTFR-2016-AVI-223 : Vulnérabilité dans Armadito Antivirus

Gestion détaillée du document

04 juillet 2016 version initiale.