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 09 janvier 2017
N° CERTFR-2017-ACT-002

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2017-ACT-002

1 - Nouvelle contre-mesure de sécurité - Arbitrary Code Guard

Aujourd'hui, la plupart des codes d'exploitation souhaitent aboutir à l'exécution d'un code arbitraire injecté dans la machine cible. Du point de vue de l'attaquant, l'avènement de contre-mesures telles que la prévention de l'exécution de données (*Data Execution Prevention* ou *DEP*) nécessite plusieurs étapes avant d'y parvenir. Il peut par exemple être nécessaire de changer les protections d'une page mémoire pour la rendre exécutable. L'idée de séparer définitivement les pages inscriptibles des pages exécutables élimine ce mode d'attaque.

Sous certains systèmes Linux, la contre-mesure *PAX_MPROTECT* (cf. Documentation [1]) de PaX implémente ce cloisonnement depuis le début des années 2000. Depuis le 7 décembre 2016, une fonctionnalité analogue (*Arbitrary Code Guard* ou *ACG* - cf. Documentation [2][3]) est utilisée par le navigateur Edge de Microsoft sous Windows 10 version 14986 (cf. Documentation [4]).

L'emploi du drapeau *ProhibitDynamicCode* associé à un processus interdit :

- l'allocation de nouvelles pages exécutables et inscriptibles ;
- le changement de protection des pages existantes pour les rendre exécutables ;
- le changement de protection des pages exécutables pour les rendre inscriptibles.

Un attaquant ne peut donc injecter sa charge utile dans une page inscriptible puis l'exécuter.

Notons que cette protection empêcherait également les compilateurs à la volée de produire du code dynamique. Ceci serait problématique dans le cadre de l'exécution de code JavaScript dont la performance est un élément essentiel de la toile 2.0.
Microsoft a donc prévu une exception permettant à un fil d'exécution de se soustraire à la règle par le biais du drapeau *AllowThreadOptOut*. Dans son état actuel, Edge utilise ce drapeau mais, dans le futur, la production de code compilé à la volée devrait être déléguée à un sous-processus renforçant ainsi la protection.

Cette innovation s'inscrit dans une série de contre-mesures déployées par Microsoft notamment dans Windows 10.

Le CERT-FR recommande l'installation des dernières mises à jour et si possible la migration vers des systèmes récents.

D'autres techniques d'exploitation ne reposent pas sur l'injection de code exécutable et les attaquants se réorienteront probablement vers celles-ci. Néanmoins, un mode d'attaque très courant est éliminé par cette contre-mesure.

Documentation

1. https://pax.grsecurity.net/docs/mprotect.txt
2. https://technet.microsoft.com/en-us/security/dn425049.aspx
3. https://www.blackhat.com/docs/us-16/materials/us-16-Weston-Windows-10-Mitigation-Improvements.pdf
4. https://blogs.windows.com/windowsexperience/2016/12/07/announcing-windows-10-insider-preview-build-14986-pc/

2 - Rappel des avis émis

Dans la période du 02 au 08 janvier 2017, le CERT-FR a émis les publications suivantes :

- CERTFR-2017-AVI-001 : Multiples vulnérabilités dans le noyau Linux de SUSE
- CERTFR-2017-AVI-002 : Multiples vulnérabilités dans Google Android (Nexus)

Gestion détaillée du document

09 janvier 2017 version initiale.