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 10 juillet 2017
N° CERTFR-2017-ACT-027

**Affaire suivie par :**
CERT-FR

# BULLETIN D'ACTUALITÉ

**Objet : Bulletin d'actualité CERTFR-2017-ACT-027**

## 1 - Recommandations concernant l'utilisation de scanneurs de vulnérabilité MS17-010

Le 14 mars 2017, le correctif MS17-010 a été publié par Microsoft afin de corriger des vulnérabilités dans l'implémentation de la version 1 du protocole SMB permettant une exécution de code privilégié à distance. Les vulnérabilités correspondantes sont communément désignées par *EternalBlue*, *EternalRomance*, *EternalChampion* et *EternalSynergy*.

Le CERT-FR note la mise à disposition sur Internet de scanneurs réseau afin de déterminer si le correctif MS17-010 est installé sur une machine, dont certains présentent un risque de sécurité pour leurs utilisateurs.

### Recherche de la présence du correctif MS17-010

Il est possible de tester l'installation du correctif MS17-010 sur une machine Windows par un scan réseau. La démarche est la suivante :

- Tenter d'établir une connexion SMB (port 445 TCP) vers l'adresse IP à tester, par exemple *192.168.0.128* ;
- Une fois la connexion établie, négocier un dialecte SMB (*NEGOCIATE*) et ouvrir une session anonyme (*SESSION_SETUP*) ;
- Réaliser une requête de connexion au partage ayant comme chemin «*192.168.0.128**IPC$*»(*TREE_CONNECT*) ;
- Réaliser une interrogation du tube nommé (*PeekNamedPipe*) «*PIPE*\»ayant un champ FID à *0x0000* ;
- Si la machine testée répond par une erreur *STATUS_ACCESS_DENIED* ou *STATUS_INVALID_HANDLE*, le correctif MS17-010 est installé et la machine n'est pas vulnérable ;
- Si la machine testée répond par une erreur *STATUS_INSUFF_SERVER_RESOURCES*, la machine n'a pas de correctif installé et est vulnérable.

Dans le cas où il existerait des mécanismes de filtrage du traffic SMB entre la machine réalisant le scan et une des machines ciblées, les résultats du test doivent être interprétés pour prendre en compte ces mécanismes.

### Recherche de la présence de la porte dérobée *DoublePulsar*, et limitations

Des outils disponibles en ligne proposent également de détecter la présence de la porte dérobée *DoublePulsar*, communément installée par les codes exploitant les vulnérabilités MS17-010.

Cette détection est réalisée à l'aide d'une requête SMB *TRANS2 SESSION_SETUP* dont le champ *Timeout* a été renseigné de manière à passer un code d'opération à la porte dérobée.

*DoublePulsar* utilisera le champ *Timeout* de la requête pour déterminer l'opération à effectuer, et le champ *MultiplexId* de la réponse pour transmettre le code de retour. Dans la version de *DoublePulsar* utilisée par le code d'exploitation *EternalBlue*, le comportement suivant est observé :

- La porte dérobée réalisera la somme modulo 256 des quatre octets du champ, dont le résultat correspond au code d'opération ;
- Le code d'opération est recherché dans un ensemble de valeurs attendues, correspondant à un test de présence, à la désinstallation de la porte dérobée, ou à l'exécution d'un code transmis par le réseau ;
- Selon le code d'opération transmis et l'exécution de l'opération, le champ *MultiplexId* de l'en-tête SMB de la réponse est modifié pour valoir le *MultiplexId* de la requête auquel on additionne, modulo 256 :
  - *0x10* en cas de succès ;
  - *0x20* en cas de paramètres invalides ;
  - *0x30* en cas d'échec d'allocation mémoire.

Dans le cas où la porte dérobée est installée, on observe donc une déviation de la valeur attendue du champ *MultiplexId* de la réponse qui devrait normalement avoir la même valeur que celui de la requête.

Bien que ce comportement puisse être recherché sur le réseau, on remarque la possibilité d'éditer le code binaire de *DoublePulsar* afin de gérer des codes d'opération arbitraires, ainsi que de changer la manière dont le champ *MultiplexId* est modifié pour renvoyer le résultat de l'opération demandée.

À titre d'exemple, voici les codes d'opération pour quelques variantes de *DoublePulsar* utilisées par des codes malveillants notables. Les opérations correspondantes sont respectivement le test de présence, la désinstallation et l'exécution de code à distance :

- EternalBlue : *0x23*, *0x77*, *0xc8* ;
- EternalRomance : *0x13*, *0x67*, *0xb8* ;
- NotPetya, ExptrWrap, ExPetya (et autres appellations) : *0xf0*, *0xf1*, *0xf2*.

Les codes de retour de *NotPetya* ont également été changés pour valoir *0x11*, *0x21* et *0x31*.

Ceci limite donc la pertinence du test de présence de la porte dérobée de certains outils, capables de détecter un nombre de variantes limité, et dont le résultat doit être considéré avec précaution.

## Risques d'utilisation des scanneurs disponibles en ligne

La mise à disposition de scanneurs réseau sur Internet peut s'accompagner de risques pour les organisations souhaitant les utiliser.

Nous prenons ici comme exemple le scanneur *EternalBlues* qui transmet des statistiques via HTTP vers le site de l'éditeur du logiciel, avec les informations suivantes :

- un identifiant aléatoire, unique pour chaque exécution ;
- le nombre total de machines scannées ;
- le nombre de machines ayant répondu au scan ;
- le nombre de machines vulnérables ;
- le nombre de machines permettant d'utiliser la version 1 du protocole SMB.

La version testée est la 0.0.0.6 (MD5 : e727f13d5e8837af5da257e440bfe678).

Il est ainsi possible pour l'éditeur, en récupérant l'adresse IP publique depuis laquelle le scan a été envoyé, de déterminer la proportion de votre infrastructure n'ayant pas déployé le correctif MS17-010.

Plus généralement, il n'est pas exclu que des outils mis à disposition publiquement soient en réalité un moyen de compromettre la sécurité du système d'information, soit en réalisant l'exploitation des machines vulnérables au cours du scan de manière silencieuse, soit en transmettant les résultats du scan à un serveur de contrôle pour préparer une attaque ultérieure.

### Recommandations

Le CERT-FR recommande :

- l'utilisation d'outils de source fiable, dont le fonctionnement et les effets de bord ont été décrits et testés avant de réaliser un scan sur l'ensemble de votre infrastructure ;
- de croiser les résultats des tests de présence du correctif MS17-010 avec une documentation à jour de l'architecture du système d'information, en particulier s'il existe des mécanismes de filtrage réseau, pour déterminer l'exhaustivité du test réalisé ;
- d'installer dès leur publication les correctifs de sécurité ;
- d'accorder une confiance modérée aux résultats des tests de présence de la porte dérobée *DoublePulsar*, dont le code binaire peut être édité par un acteur malveillant pour modifier le comportement qui est recherché par les outils, et ainsi échapper à la détection.

#### Documentation

- Avis CERT-FR CERTFR-2017-AVI-082
  http://cert.ssi.gouv.fr/site/CERTFR-2017-AVI-082/index.html
- Bulletin de sécurité Microsoft du 14 mars 2017
  https://technet.microsoft.com/fr-fr/library/security/MS17-010

## 2 - Rappel des avis émis

Dans la période du 03 au 09 juillet 2017, le CERT-FR a émis les publications suivantes :

- CERTFR-2017-AVI-197 : Multiples vulnérabilités dans SCADA les produits Siemens
- CERTFR-2017-AVI-198 : Multiples vulnérabilités dans SCADA les produits Schneider
- CERTFR-2017-AVI-199 : Vulnérabilité dans ISC BIND
- CERTFR-2017-AVI-200 : Multiples vulnérabilités dans SCADA les produits Siemens
- CERTFR-2017-AVI-201 : Multiples vulnérabilités dans Joomla!
- CERTFR-2017-AVI-202 : Multiples vulnérabilités dans les produits Cisco
- CERTFR-2017-AVI-203 : Multiples vulnérabilités dans Google Android (Nexus)
- CERTFR-2017-AVI-204 : Multiples vulnérabilités dans PHP

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

- CERTFR-2017-ALE-012 : Campagne de maliciels prenant l'apparence d'un rançongiciel à multiples capacités de propagation (clôture de l'alerte.)

## Gestion détaillée du document

**10 juillet 2017** version initiale.