



Forum: Sécurité

Topic: Eternal Blues – Un scanner pour débusquer les machines vulnérables à la faille SMBv1 utilisée par Wa

Subject: Re: Eternal Blues – Un scanner pour débusquer les machines vulnérables à la faille SMBv1 utilisée par Wa

Publié par: GillesD

Contribution le : 03/07/2017 10:30:16

-message modifié sur base des informations du 03/07/2017-

Je me permets 2 petites remarques concernant ce programme :

1) ce programme scanne le sous-réseau dans lequel il est exécuté. C'est une pratique considérée comme agressive par un gestionnaire de réseau d'entreprise car fréquemment utilisée par des virus. Je déconseille donc de l'utiliser dans un réseau d'entreprise sans l'accord du responsable de la sécurité réseau.

2) l'auteur du programme a expliqué son fonctionnement, ce qui invalide la précédente version de mon post et la remarque de Korben : "Méfiance tout de même, cet outil cherche la présence active du protocole SMBv1. Donc même si vous avez patché vos machines, mais pas désactivé SMBv1, la machine sera vu comme à risque. Un faux positif donc." Ce scanner teste bien spécifiquement la vulnérabilité utilisée par Wanacry et consorts.

Par contre suite de la remarque de Korben reste aussi pertinente :

"Pensez donc aussi à désactiver SMBv1 si vous n'en avez pas l'usage."

Concrètement si le scanner ne trouve aucun problème c'est en ordre.

S'il renseigne une alerte, il faut vous assurer que ces appareils ont bien reçu tous les correctifs de sécurité de Microsoft.

Enfin, comme suggéré, le plus sûr consiste à **désactiver le protocole SMBv1** car il y a peut-être encore d'autres failles liées à ce protocole mais pas encore connues. **Attention** cependant, ce protocole est indispensable au fonctionnement en réseau de certains appareils :

- PCs sous Windows XP
- PCs sous Windows 2000 et 2003 serveur
- anciens appareils connectés directement au réseau comme des scanners, imprimantes, copieurs multifonctions