Parc d'Activités Schweitzer
26 rue du Bois Fossé
85300 CHALLANS
Tél. 02 51 49 31 31

espace technologie

ARTICLE DE PRESSE

Prévisions Vulnérabilités Fin 2019

Article écrit par Jérôme V.

Diplômé en cyber sécurité (Université Central Supelec)

Responsable des services de sécurité informatique chez Espace Technologie.

LA FAILLE CRITIQUE TOUCHANT LES ENVIRONNEMENTS MICROSOFT EN 2019

La sécurité informatique est devenue un enjeu majeur pour les entreprises. Et, pour bien vous faire comprendre en quoi cela est crucial, je vais revenir sur la faille qui a agité le monde de la Cyber sécurité cet été. Elle répondait au doux nom de Bluekeep.

Historique des failles informatiques

Revenons en arrière, suite à la publication de failles majeures des systèmes d'exploitation Windows.

En 2008, une faille se nommant MS08-067 a été publiée.

- Peu de temps après, elle a été à l'origine du ver Conficker, qui a infecté presque 9 000 000 d'ordinateurs.

Plus récemment en 2017, une faille nommée Ethernalblue a été rendu publique. Elle a permis au fameux virus Wannacry de faire d'énormes dégâts dans les entreprises.

- Des variantes de ce programme ont été déclinées en plusieurs ransomwares*. Ces deux premières failles ciblaient principalement le protocole de partage de fichiers (SMB**).

Il est plus compliqué pour un attaquant externe de se répandre sur un réseau car le protocole SMB n'est pas ouvert sur internet.

Pourtant l'histoire a prouvé que les attaques ont pourtant bien fonctionnées. (Notamment par un vecteur de mail frauduleux).

*Ransomware : Un ransomware, ou rançongiciel en français, est un logiciel informatique malveillant, prenant en otage les données. Le ransomware chiffre et bloque les fichiers contenus sur votre ordinateur et demande une rançon en échange d'une clé permettant de les déchiffrer

* *Le protocole SMB (Server Message Block3) est un protocole permettant le partage de ressources (fichiers et imprimantes) sur des réseaux locaux avec des PC sous Windows.

La faille Bluekeep et ses caractéristiques

Aujourd'hui, nous avons affaire à Bluekeep.

Il est à présager, dans un future proche, qu'une nouvelle vague de virus va se répandre.

- Le 13 juin 2019, près d'un million de systèmes semblaient concernés.

  Cette faille s'attaque au protocole RDP.

  C'est la technologie qui est mise en place pour se connecter à un serveur à distance.

  De ce fait, la méthode de propagation est différente car elle ne passe pas forcément par une première attaque de phishing (mailing frauduleux), mais cible directement les serveurs ouverts sur internet.

  Elle permet l'exécution d'un code à distance, ce qui permet à l'attaquant de s'implanter dans les systèmes d'informations des entreprises.

- Le 13 août 2019, les vulnérabilités de sécurité BlueKeep associées, appelées collectivement **DejaBlue**, affectaient l'ensemble des systèmes d'exploitation Windows.
- Le 6 septembre 2019, un exploit (un code d'exploitation) de la vulnérabilité de sécurité liée au ver BlueKeep a été annoncé et rendu public.

La NSA* a recommandé des mesures supplémentaires, telles que la désactivation des services de bureau à distance et de son port associé s'ils n'étaient pas utilisés, ainsi que de l' authentification au niveau du réseau (NLA) pour RDP**. Cependant, la meilleure protection consiste à déconnecter RDP d'Internet. Désactivez RDP s'il n'est pas utilisé et, si nécessaire, rendez RDP accessible uniquement via un réseau privé virtuel (VPN***) .

*National Security Agency

**Remote Desktop Protocol est un protocole qui permet à un utilisateur de se connecter sur un serveur exécutant Microsoft Terminal Services

***un réseau privé virtuel, abrégé VPN – Virtual Private Network, est un système permettant de créer un lien direct entre des ordinateurs distants, qui isole leurs échanges du reste du trafic se déroulant sur des réseaux de télécommunication publics.

Les recommandations d'Espace technologie

- Tous les serveurs ayant le port 3389* directement ouvert sur internet doivent impérativement être désactivés et s'orienter vers des solutions de types VPN ou passerelle SSL.

Attention : Les éditeurs de logiciel ou certains prestataires ont pour habitude d'ouvrir ce port pour assurer la maintenance. Nous vous conseillons vivement de vous assure que ce port est fermé

- Tous les postes ou serveurs plus anciens que Windows serveurs 2012 et Windows 7 doivent être migrés en version récente. Vérifier que chaque poste est bien à jour avec les derniers patchs de sécurité délivrés par Windows Update. De plus il est fortement recommandé de mettre en place une technologie de type UTM (SonicWall/Sophos) ayant la fonction IPS activée sur la patte WAN (internet) et LAN (réseau local) afin d'être proactif sur la détection de charge malveillante.

*Le protocole RDP (port par défaut 3389) est couramment utilisé dans le monde professionnel pour accéder à des bureaux distants.

** SSL Transport Layer Security ou Sécurité de la couche de transport, et son prédécesseur Secure Sockets Layer, sont des protocoles de sécurisation des échanges sur Internet.

Jerome V. RSSI Espace technologie
(Responsable Sécurité des systèmes d'information)

Plus d'informations sur nos prestations contactez-nous :

ESPACE TECHNOLOGIE
Parc d'Activités Schweitzer
26 rue du Bois Fossé - BP 147
85301 CHALLANS Cedex
Tél. 02 51 49 31 31
www.espace-technologie.com
contact@espace-technologie.com