AGENCE NATIONALE DES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION

Centre d'Alerte et de Réponse et
Aux Incidents de Sécurité Informatique

NATIONAL AGENCY FOR INFORMATION AND COMMUNICATION TECHNOLOGIES

Computer Incident Response Team

ALERTE DE SECURITE

Faille de sécurité BlueKeep

Contenu

I. Contexte

Ce n'est pas la première ni la dernière faille détectée sur Windows. Après le célèbre WannaCry qui menace encore des milliers d'ordinateurs dans le monde, la dernière menace agitée par Windows se nomme BlueKeep. Il s'agit pour l'instant d'une faille encore non exploitée. Mais son usage éventuel par des pirates pourrait avoir de terribles conséquences.

Microsoft a rappelé aux utilisateurs que WannaCry n'a été diffusé que deux mois après la publication de MS17-010, la mise à jour qui corrigeait la vulnérabilité exploitée par WannaCry. Elle résidait dans SMBv1, une version ancienne du protocole qui permet à un ordinateur de partager des fichiers et des répertoires avec d'autres ordinateurs. Les experts en sécurité utilisent le terme « wormable » pour décrire la vulnérabilité en raison de sa capacité à déclencher des vers, qui sont des logiciels malveillants se reproduisant sur plusieurs ordinateurs en utilisant un réseau informatique comme Internet. Ils ont la capacité de se dupliquer une fois qu'ils ont été exécuté. Contrairement au virus, le ver se propage sans avoir besoin de se lier à d'autres programmes exécutables

II. Fonctionnement

La faille wormable BlueKeep, quant à elle, provient en revanche d'un bogue de type « dangling pointers » dans les services Bureau à distance, qui fournit une interface graphique pour la connexion à un autre ordinateur via Internet. Les « dangling pointers » sont des pointeurs qui ne pointent pas vers un objet valide du type approprié. Ce sont des cas spéciaux de violations de la sécurité de la mémoire. Cette vulnérabilité dite BlueKeep, fait officiellement l'objet d'un suivi en tant que CVE-2019-0708.

Les exploits qui en découlent peuvent exécuter de manière fiable du code malveillant sans interaction de la part d'un utilisateur final. La gravité de la situation a incité Microsoft à émettre des correctifs inhabituels pour Windows 2003, XP et Vista, qui n'étaient plus pris en charge depuis quelques années.

La vulnérabilité CVE-2019-0708 nécessite une attaque à faible complexité pour être exploitée. Le système d'évaluation de vulnérabilité de Microsoft évalue cette complexité à 3,9 sur 10. Pour plus d'éclaircissements, les développeurs de WannaCry possédaient un puissant code d'exploitation qui a été développé par la National Security Agency - et qui lui a été volé - afin d'exploiter les "wormable" CVE-2017-0144 et CVE-2017-0145, où la complexité des exploitations était qualifiée "d'élevée". Il faut donc comprendre que développer un code d'exploitation fiable pour cette dernière vulnérabilité Windows nécessitera relativement peu de travail.

L'exploitation de la vulnérabilité, nécessiterait simplement que quelqu'un envoie des paquets spécifiques sur le réseau à un système vulnérable disposant du service RDP.

III. Comment se protéger ?

Nous recommandons à toute personne utilisant un ordinateur vulnérable de se mettre à jour immédiatement. La faille affecte les versions de Windows XP à Server 2008 R2. Toute personne utilisant l'une de ces versions doit s'assurer qu'un correctif est appliqué.

Il faut également vérifier que RDP (Remote Desktop Protocol) n'est pas exposé à Internet, sauf en cas de nécessité absolue. L'activation de l'authentification au niveau du réseau pour les services de postes de travail distants est une mesure utile, mais elle est inefficace contre les attaquants possédant des mots de passe réseau, ce qui est fréquent dans les infections par ransomware. Windows 8 et 10 ne sont pas affectés.

lien pour télécharger le correctif sur Windows 7, Windows 2008 R2 et Windows 2008

lien pour télécharger le correctif sur Windows 2003 et Windows XP