Quand un fichier Windows infecte l'environnement Linux [MAJ]

Les fichiers malveillants exécutables sous Windows ne se limitent pas à l'environnement de Microsoft. Contre toute attente, ils peuvent aussi faire des dégâts sur un système Linux. C'est du moins ce qu'a découvert l'expert en sécurité Nils Dagsson Moskopp à propos des fichiers MSI. Cet installateur Windows peut lancer du code malveillant sur les ordinateurs équipés d'une distribution Linux à cause d'une vulnérabilité de l'environnement Open Source que le chercheur a baptisée «Bad Taste» (mauvais goût), et qui est référencée CVE-2017-11421.

La faille réside dans le composant gnome-exe-thumbnailer. Lequel est utilisé par le gestionnaire de fichiers de Gnome (un des environnements de bureau GNU/Linux parmi les plus populaires) pour générer les vignettes des fichiers dans l'environnement graphique selon la nature du format concerné. Pour déterminer le programme associé, le gestionnaire de fichiers proposé dans Gnome (comme Nautilus chez Ubuntu) analyse automatiquement les fichiers du répertoire afin d'extraire une icône de son contenu et l'afficher à l'écran. Par exemple, les fichiers vidéo montreront une imagette issue du film.

Du VBScript lu par Linux

Fort de cette caractéristique, le chercheur en sécurité s'est rendu compte qu'il pouvait glisser un VBScript malveillant dans le nom d'un fichier MSI, comme il le démontre sur sa publication. A la lecture du fichier MSI, l'explorateur du fichier exécute le code qui se trouve dans le nom. Dans sa démonstration, le chercheur s'est contenté de provoquer la création du fichier badtaste.txt, vide en l'occurrence. Mais, selon lui, un acteur moins bienveillant pourrait générer des actions bien plus dommageables pour l'utilisateur de la machine.

Il lui faudrait cependant réussir à lui faire télécharger le fichier MSI infectieux en question. Les techniques d'attaques par ingénierie sociale ne manquent certes pas pour y parvenir. Notamment via la technique dite de « Drive-by-download » qui installe automatiquement un fichier à la consultation d'une page web ou d'un e-mail. Si tant est que le navigateur ou le client de messagerie n'en demande pas la validation par l'utilisateur. Qui plus est, l'exécution de code malveillant s'inscrira dans les limites des droits d'administration de l'utilisateur. Pour exploiter le plein potentiel du système, l'attaquant devra parvenir à obtenir les droits administrateur (root).

Faille corrigée

Pour se prémunir des hypothétiques conséquences de cette vulnérabilité Bad Taste, le chercheur invite les utilisateurs à supprimer tous les fichiers du répertoire '/usr/share/thumbnailers' où sont stockés les éléments de configuration des générateurs de vignette. Suppression qu'il faudra évidemment effectuer en ligne de commande et non pas en utilisant un gestionnaire de fichiers graphique. Dans tous les cas, Nils Dagsson Moskopp a informé les développeurs du projet Debian (à partir duquel sont développées nombre de distributions Linux dont Ubuntu) de la vulnérabilité.

Laquelle est aujourd'hui corrigée. Les utilisateurs de l'environnement Open Source qui mettent régulièrement à jour leur OS sont donc protégés.

[Mise à jour à 17:40] Un lecteur bien avisé nous fait remarquer que la vulnérabilité n'est exploitable sous l'environnement Gnome uniquement si Wine est bien installé. Ce composant permet d'exploiter des programmes Windows sous Linux et n'est pas installé par défaut dans les principales distributions. Il ajoute également que, au-delà de la mise à jour de l'OS corrigé, la correction provisoire n'est pas de supprimer tous les fichiers du répertoire '/usr/share/thumbnailers' comme nous avions cru l'avoir compris mais de faire un :
sudo chmod -x /usr/bin/gnome-exe-thumbnailer.

Lire également

[Un malware Linux force les Raspberry Pi à miner de la crypto-monnaie]

[L'OS Linux Ubuntu s'invite sur le Windows Store de Microsoft]

[Stack Clash s'octroie des privilèges sur les systèmes Linux]