Les plug-ins Java et Flash sous contrôle dans EMET 5.0 de Microsoft

Si les cybercriminels ont de la ressource et de l'imagination, les acteurs IT tentent de répondre aux attaques variées avec différents types d'outils. Microsoft dispose par exemple d'une solution pour atténuer les effets des attaques et notamment de celles utilisant des failles zero day.

Nommée EMET (Enhanced Mitigation Experience Toolkit), celle-ci vient de passer en version 5.0. Un aperçu de la mouture avait été donné il y a 6 mois, lors de la conférence RSA, avec la présentation de deux services garantissant le contrôle des plug-ins et la protection de la mémoire. Le premier, baptisé ASR (Attack Surface Reduction), donne aux administrateurs de Windows la possibilité de **déterminer quand et si les plug-ins Java et Flash doivent être intégrés à Windows**. Ces deux plateformes sont souvent la cible préférée des pirates qui s'en servent comme porte d'entrée pour leurs attaques. Avec ASR, les administrateurs peuvent autoriser l'usage de plug-in Java pour les sites web internes, tout en les bloquant pour l'accès à Internet. De même, ils peuvent empêcher les applications Office de charger Flash dans un document Word ou Excel tout en l'autorisant dans le navigateur.

« *Nous avons entendu les utilisateurs qui souhaitaient obtenir plus de contrôle sur les programmes et sur les scénarios où les plug-ins peuvent être chargés. Nous avions d'abord publié un outil Fix It l'année dernière pour désactiver complétement* le plug-in Java dans Internet Explorer, ce qui a aidé les gens », explique Jonathan Ness, directeur du développement sécurité pour Microsoft Security Response Center. Il ajoute : « *mais les clients nous ont expliqué qu'ils avaient encore besoin de Java pour leurs applications métiers fonctionnant sur leur Intranet local et ils cherchaient un moyen de bloquer Java et d'autres plug-ins uniquement sur Internet* ».

Prévention et surveillance améliorée

L'autre service d'atténuation dans EMET 5.0 se nomme EAF + (pour Export Address Table Filtering Plus) qui introduit de **nouvelles méthodes pour enrayer les attaques avancées**. « *L'EAF + ajoute une protection dite 'page de garde' pour aider à prévenir les opérations sur la lecture mémoire couramment utilisées pour les fuites de données* ».

Microsoft a également **modifié les options de configuration dans EMET 5.0**. Il donne la possibilité aux administrateurs de paramétrer davantage les mesures d'atténuation. « *Il est possible par exemple de configurer la protection d'adresses mémoires spécifiques avec Hearspray Allocation depuis EMET 5.0*, précise le dirigeant. *De plus, les modifications de paramétrages peuvent être intégrées dans les règles de groupes d'Active Directory. Les administrateurs peuvent ainsi pousser les modifications sur un ou la totalité des utilisateurs* ». Enfin, EMET 5.0 intègre d'autres services comme un **tableau de surveillance des activités suspectes** et la gestion des certificats de confiance. La dernière version d'EMET est disponible en téléchargement depuis cette page.

A lire aussi :

Sécurité : Microsoft Active Directory victime d’une faille critique

Microsoft met fin à ses alertes de sécurité par email