Une faille «zero day» de SharePoint expose les données des entreprises

Les données des entreprises circulant sur les plates-formes SharePoint sont-elles en danger? C'est à craindre. Jeudi 29 avril, Microsoft a émis un avis de sécurité concernant une vulnérabilité qui touche **Windows SharePoint Services 3.0 et Office SharePoint Server 2007**, en éditions 32 comme 64 bits. Les autres déclinaisons de SharePoint ne sont pas affectées.

Révélée à l'éditeur de Redmond le 12 avril dernier par la société de sécurité suisse **High-Tech Bridge** (qui a développé un code de démonstration pour l'occasion), la faille est d'autant plus inquiétante qu'elle ne dispose pas pour l'heure de correctif. Dite «zero day», la brèche de sécurité exploite une méthode de *cross site scripting* (XSS) qui, bien menée, permet à l'attaquant de disposer des privilèges du compte utilisateur. En ciblant bien sa proie, le cybercriminel pourrait potentiellement accéder aux informations qui circulent sur l'intranet de l'entreprise.

*« Le scénario le plus probable est qu'**un attaquant envoie un liens malfaisant à un utilisateur connecté au serveur Sharepoint***, explique l'équipe *Security Research & Defense* sur son blog. *Si l'utilisateur clique sur le lien, le code JavaScript de l'attaquant et embarqué dans le lien serait exécuté dans l'environnement de l'utilisateur. »*

S'il n'existe aucun correctif (ni aucune attaque signalée), Microsoft n'en fournit pas moins **quelques conseils** pour éviter les éventuels désagréments imputables à la vulnérabilité. L'éditeur invite notamment les administrateurs à activer la fonction de filtrage XSS d'IE8, y compris pour la zone intranet.

Autre solution de contournement recommandée par Microsoft, **la restriction d'accès au fichier SharePoint Help.aspx** qui ne pourra donc pas être utilisé par le pirate éventuel… ni pas l'utilisateur. Un palliatif en attendant le correctif.