Project Zero : Google lâche du lest sur les failles Zero Day

Le Project Zero, qui voit des ingénieurs de Google étudier le code de tous types de logiciels pour y dénicher des vulnérabilités, assouplit ses règles de divulgation des failles de sécurité informatique non corrigées, et potentiellement exploitables, dites failles «zero day». Selon la nouvelle politique énoncée vendredi dernier par voie de blog, l'équipe du projet accordera un délai de 14 jours supplémentaires à tout éditeur qui fera savoir à Google qu'il est sur le point de sortir son correctif de sécurité. Concrètement, cela allongera de deux semaines la durée de rétention de l'information, jusqu'alors fixée à 90 jours.

Autre évolution, les failles zero day ne seront plus divulguées la veille d'un jour non ouvré (week-end, jour férié aux Etats-Unis) mais attendront le prochain jour travaillé pour être rendues publiques. Enfin, Google vérifiera également que les CVE (la norme permettant d'assigner une référence unique à chaque faille de sécurité) auront bien été pré-assignées pour les failles dépassant la période de rétention de l'information. Une manière d'éviter toute confusion sur la faille désignée, selon Google.

Accélérer l'édition des correctifs

Rappelons que, créé en juillet 2014, le Project Zero réunit une équipe de chercheurs en sécurité qui s'attache à scruter les bugs informatiques afin de renforcer l'intégrité des applications. Quand les experts trouvent une faille, ils en informent l'éditeur et lui accordent un délai de 90 jours pour la corriger avant de la rendre publique, preuve à l'appui. Une pratique qui *« améliore la sécurité de l'utilisateur final en accélérant l'édition des correctifs »*, souligne Chris Evans, membre du projet.

Mais une méthode qui, début janvier, avait provoqué l'ire de Microsoft alors que Google avait dévoilé une faille non corrigée, depuis 90 jours au moins, de Windows 8.1. Ce qui n'avait pas empêché Google de révéler, toujours selon la règle des 90 jours, une autre faille zero day dans Windows (7 et 8.1). Quelques jours après la colère de Microsoft, qui appelait à une meilleure coordination entre les éditeurs.

Microsoft opposé au Project Zero

Si l'éditeur de Redmond a apprécié l'assouplissement de la règle de Google, il n'en reste pas moins opposé au Project Zero. *« Alors que nous accueillons positivement les ajustements sur les pratiques de divulgation, nous sommes en désaccord avec les délais arbitraires car chaque problème de sécurité est unique et la période de mise à jour et de test varie »*, a déclaré Chris Betz aux médias américains. Le responsable du Microsoft Security Response Center (MSRC) met en avant le fait que, si l'on révèle une faille avant son correctif *« le risque d'attaque s'élève pour les utilisateurs »*.

Microsoft feint ainsi d'oublier que ces délais de divulgation ont justement pour objet de pousser les éditeurs à accélérer leurs développements pour corriger les vulnérabilités et mieux protéger leurs

clients, et éviter de laisser des brèches en jachère. De plus, l'éditeur de Windows semble s'inscrire en porte-à-faux vis-à-vis de ses confrères en matière de temps de correction. Sur les 154 failles étudiées par le Project Zero (qui concernent tout autant les produits maison Chrome et Android), 85% ont été corrigées dans le délai des 90 jours fixé arbitrairement. Un taux qui monte à 95% depuis octobre 2014. Adobe, star s'il en est en matière de vulnérabilités avec Flash Player notamment, a corrigé 100% des 37 brèches de sécurité découvertes dans le cadre du Project Zero en temps et en heure. Un exemple à suivre.

Lire également

Sécurité : Google subventionne la recherche de vulnérabilités
Faille Zero Day : Et de trois pour Flash Player !
Une faille zero day exploitée dans Windows pour cibler l'OTAN