Project Zero revoit sa stratégie de sa « chasse aux failles »

Chez Project Zero, la « politique des 90 jours » n'est plus. En tout cas sous sa forme historique. Google a décidé d'un assouplissement. Le temps de clarifier une notion qu'il estime « mal comprise ».

Cette notion, c'est la séparation des phases de développement et d'adoption des correctifs de sécurité. Jusqu'ici, elle était implicite. Tout éditeur auquel Project Zero rapportait une faille avait, de manière générale, 90 jours pour la colmater* avant qu'elle soit rendue publique avec les détails techniques. Il était censé inclure, dans ce délai, le temps nécessaire aux utilisateurs pour installer le patch. Cela ne s'est globalement pas réalisé, déplore Google.

Dans ce contexte, la politique de Project Zero subit trois changements majeurs.

- Jusqu'alors, on révélait les failles et les détails techniques 90 jours après signalement. Désormais, **pour celles corrigées dans les délais, les détails techniques ne seront publiés que 30 jours après**. Rien ne change pour celles qui n'auront pas fait l'objet d'un correctif. La « période de grâce » de 14 jours accordable en cas de capacité à patcher sous 104 jours reste par ailleurs valable.
- Les **failles activement exploitées** étaient jusqu'alors rendues publiques 7 jours après leur signalement, sans période de grâce. Dorénavant, il existe une période de grâce de 3 jours. Et Project Zero **attendra, là aussi, 30 jours pour publier les détails techniques**.
- Sous l'ancienne politique, **en cas de mise en œuvre de la période de grâce**, correctif et détails techniques faisaient l'objet d'une publication simultanée. À partir de maintenant, **ce sera également à J +30**, déduction faite des jours utilisés sur la période de grâce.

Reculer pour mieux sauter ?

Parmi ce qui ne change pas, on aura noté le cas des variantes. Leur signalement restera immédiat, au sein du même rapport que la faille principale.

Passer à du « 60 + 30 » serait trop brusque, admet Google. La « légère régression » pour laquelle le groupe américain a opté appelle toutefois un réajustement progressif. Première étape : « 84 + 28 » l'an prochain. Il s'agira de conserver des valeurs divisibles par 7 pour réduire les chances que les dates butoir tombent un week-end.

Pour aller plus loin sur les contributions de Project Zero :

- Les failles 0-day se suivent… et se ressemblent (février 2021)
- iPhone : quelle est cette faille Wi-Fi qui fait le buzz ? (décembre 2020)
- Avast : porte ouverte au code malveillant ? (mars 2020)
- Piratage : les voies de l'iPhone ne sont pas impénétrables (août 2019)
- Ces antivirus au service des pirates (juillet 2016)
- Des mots de passe se perdent chez Trend Micro (janvier 2016)

- ESET se dépêtre d'une faille critique (juin 2015)

** L'an dernier, Google avait affirmé que 97,7 % des signalements de Project Zero donnaient lieu à une correction sous 90 jours. Il avait fait évoluer sa politique sur un point en particulier : la gestion des correctifs incomplets.*

Photo d'illustration © isaak55 – Shutterstock