

Un chasseur de ' bugs ' annule son projet de révélations sur Oracle

Nommé Cesar Cerrudo, ce « *trappeur du bug* » dont les révélations sur les failles dans les solutions d'Oracle étaient très attendues a simplement expliqué avoir découvert de « *nombreux problèmes* ». Le mystère reste donc entier quant à la nature de ces vulnérabilités. Coup de bluff?

Dans une note publiée sur le site de sa société, Cesar Cerrudo, créateur de la société argentine de sécurité : Argeniss Information Security, explique que, finalement, il ne fera pas de révélations.

Cerrudo en profite pour s'excuser auprès des amateurs de sécurité et de scoop, mais aussi auprès des contributeurs qui l'ont aidé à analyser les solutions d'Oracle à la recherche de failles. Seulement, il ne donne pas plus de détails sur les raisons de cette annulation.

Dans un commentaire publié sous la note, Cerrudo écrit à propos de ce choix :« *je suis triste et énervé* » mais il précise qu'il préfère ne pas s'expliquer pour ne pas « *causer plus de problèmes* ». Une réflexion que d'aucuns jugeront, « *curieuse* », le chercheur aurait-il été la cible de pressions? Pour l'instant, rien ne le prouve, mais ses déclarations laissent planer dans l'air, un parfum de déjà vu.

Cerrudo aurait été inspiré par une autre initiative de chercheurs indépendants dont silicon.fr s'est fait l'écho : le Month of Kernel Bugs.

Avant ce brusque retournement de situation Cerrudo expliquait ses motivations : » *Nous voulons montrer ou en est le niveau de sécurité des logiciels d'ORacle, et démontrer que dans ce*

domaine Oracle n'avance pas. »

D'après Cerrudo, sa société Argeniss pourrait tenir une année entière à montrer les bugs dans les solutions de l'éditeur.

Rappelons que les failles dites « Zero-day » sont celles qui ne sont pas corrigées par le revendeur. La publication de ces découvertes avant l'apparition d'un correctif a le don d'agacer l'industrie. Cette pratique a considérablement augmenté la bisbille entre les chercheurs de vulnérabilité et les revendeurs de logiciels.

Exemple: en 2005, Sybase a menacé de poursuivre Surrey une société de sécurité qui souhaitait publier sur la Toile les détails de huit failles dans ses logiciels. Pourtant, ces bugs étaient corrigés. On imagine la réaction d'Oracle à l'annonce de la publication de Cerrudo.

Même si rien ne prouve l'existence de pressions, on connaît le point de vue d'Oracle sur les chercheurs indépendants. Sur son blog le groupe explique que « *la publication des failles zero-day est un comportement irresponsable, car cela met en péril nos clients. »*