Une faille dans l'intégration d'OAuth 2.0 et OpenID touche les acteurs du web

Depuis la découverte de la faille Heartbleed, le monde du web se penche sur la fiabilité et la sécurisation de certaines solutions Open Source, notamment dans le domaine de la sécurité des communications. **Dans la loi des séries, un chercheur vient de découvrir une vulnérabilité dans la mise en place de deux protocoles d'authentification** OAuth 2.0 et OpenID, utilisés par de nombreux acteurs du web. Ces deux protocoles permettent l'authentification d'un site web utilisant l'API sécurisée d'une autre application ou via des vérifications de jeton sur un serveur. Ainsi, l'utilisateur peut depuis son compte Facebook avoir accès à des services d'autres sites web sans avoir besoin de s'identifier à nouveau.

Récupérer des informations sensibles

Wang Jing, doctorant l'Université technologique de Nanyang à Singapour, explique dans une page web que cette faille touche plusieurs grands sites comme Facebook, Google, Linkedin ou Microsoft (principalement la plateforme Live). **La vulnérabilité facilite une attaque connue sous le nom « Covert Direct »** (redirection secrète) qui donne son nom à la faille découverte. L'objectif est d'orienter l'utilisateur vers un site malveillant et de lui présenter une fenêtre avec un module d'authentification ressemblant aux sites connus (Facebook, Linkedin, etc.) pour récupérer ses identifiants et ensuite s'en servir sur d'autres sites. Wang Jing explique qu' OAuth et OpenID ne parviennent pas à vérifier correctement les URL. « *En donnant une autorisation avec d'importants privilèges, l'attaquant peut* ***obtenir des informations plus sensibles comme les messages de la boîte mail, la liste de contacts et leur présence en ligne et même gérer le compte***», constate l'universitaire chinois.

Une solution : la liste blanche

Il indique dans son blog avoir trouvé la vulnérabilité en février dernier avant de la signaler aux différents acteurs. Il admet que le travail sur un patch *« est plus facile à dire qu'à faire »*. Pour autant, il existe **une solution avec la mise en place d'une liste blanche** où des sites tiers doivent s'enregistrer s'ils veulent que les utilisateurs puissent interagir avec leurs API. Cette solution a été intégrée par Linkedin. Pour les autres sites sollicités par Wang Jing, Google lui a indiqué qu'il enquêtait sur le problème. Microsoft a identifié ce problème sur un site tiers. Yahoo n'a pour l'instant pas répondu à la notification du chercheur chinois.

Pas de nouvelle faille Heartbleed, selon les spécialistes

Pour autant, l**a communauté des experts en sécurité se garde bien de faire un parallèle entre cette faille et celle de Heartbleed** dans la librairie Open SSL. Pour Dany Thorpe, architecte

sécurité chez Dell, *« il ne s'agit pas d'une vulnérabilité dans OAuth lui-même »*. Le site Mashable estime que l'attaque présentée n'est pas nouvelle et évoque une méthode similaire découverte en mars 2013 par le consultant Egor Homakov. Pour Symantec, il n'y a pas d'équivoque, « *la faille Covert Direct dans OAuth n'est pas le prochain Heartbleed »,* peut-on lire sur le blog de l'éditeur et d'ajouter que « ***la faille est dans l'implémentation d'OAuth par les fournisseurs de service*** ».

Lire également

Sécurité : 91 % des services Cloud utilisés en Europe présentent un risque