Cupidon injecte la faille Heartbleed dans les routeurs WiFi et Android

En sismographie, on appelle cela les répliques. Il y a 7 semaines le monde découvrait une faille répondant au nom de Heartbleed. La vulnérabilité référencée CVE-2014-0160 permet à des pirates d'accéder aux informations personnelles (jusqu'à 64 Ko de données) et chiffrées des utilisateurs lors de transactions en ligne. Le trou de sécurité touche le logiciel OpenSSL chargé de protéger login de connexion, mot de passe, numéro de carte bancaire et autres données depuis le serveur qui héberge la transaction en cryptant la communication réalisée depuis le terminal (PC, tablette, smartphone…) sous protocole **SSL/TLS**.

Or depuis la découverte de la faille, éditeurs et constructeurs ont rapidement travaillé pour apporter des correctifs à cette vulnérabilité. Une grande majorité des produits sont maintenant à l'abri, même si une étude récente montrait qu'environ 320 000 serveurs étaient encore vulnérables. De manière assez régulière, des constructeurs avertissent leurs clients sur la mise en place de correctifs liés à Heartbleed. C'est le cas notamment de Schneider Electric qui a listé les produits vulnérables.

Une méthode baptisée Cupidon

Aujourd'hui, c'est un chercheur en sécurité portugais, Luis Grangeia, qui publie une méthode d'attaque s'appuyant sur **Heartbleed via les réseaux WiFi et les terminaux Android**. De manière assez poétique, le chercheur a baptisé son attaque, **Cupidon**. Il a utilisé la faille dans OpenSSL mais dans un environnement WiFi fermé (notamment en entreprise). Concrètement, il explique que les réseaux sans fil d'entreprise utilisent des tunnels TLS pour sécuriser une partie des processus d'authentification (EAP). Il a donc créé un patch pour le logiciel de sécurisation du WiFI, **WPA supplicant** et le logiciel de création de point d'accès WiFi, **Hostpad**. Cupidon permet de capturer les informations transitant entre le routeur et le terminal.

Sur le terminal, le chercheur indique que « les appareils sous **Android 4.1 (Jelly Bean)** sont particulièrement vulnérables » et appelle donc les utilisateurs à mettre à jour leurs mobiles ou tablettes. Mais dans sa présentation, Luis Grangeia évoque des risques sur d'autres appareils qui pourraient utiliser **OpenSSL pour les tunnels TLS EAP** et de citer avec un point d'interrogation **iOS et MacOS X**. Les solutions WiFi sont bien évidement pointées du doigt avec Cisco/Merkai, Aruba, Trapeze, etc, mais pas seulement les téléphones sur IP ou les imprimantes peuvent être impactées par cette attaque.

La Core Initiative Infrastructure investit sur la sécurité des projets Open Source

Cette nouvelle méthode d'attaque montre les besoins en sécurité des projets Open Source. Les grands acteurs de l'IT (Microsoft, Facebook, Google et plus récemment Salesforce ou Adobe) se sont mobilisés pour apporter leur aide technique et financière dans la sécurisation et les tests des projets Open Source critiques. La Core Initiative Infrastructure, présidée par la Fondation Linux, vient de dresser **la liste des projets prioritaires**. Sans surprise, **OpenSSL** arrive en tête après l'affaire Heartbleed. On constate également que l'accent va porter sur **OpenSSH et le Network**

Time Protocol (NTP). Ce dernier inquiète particulièrement les spécialistes en sécurité par son usage dans les récentes attaques DDoS par amplification.

A lire aussi :

Faille Heartbleed : la check-list pour s'en sortir

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