Open SSL : une faille critique à colmater rapidement

Les administrateurs de serveurs sont invités à se tenir prêts pour installer, ce jeudi 9 juillet, la dernière mise à jour d'OpenSSL, qui corrige une faille dite « hautement critique ». Pour éviter de donner des indices aux pirates, l'équipe chargée de maintenir la bibliothèque open source de chiffrement n'entre pas dans les détails au sujet de cette vulnérabilité qui peut notamment être exploitée pour lancer des attaques par déni de service (DoS).

Tout au plus sait-on que les implémentations les plus « classiques » d'OpenSSL peuvent être touchées. Y compris par l'exfiltration de données stockées dans la mémoire du serveur ou par l'exécution de code à distance. Si les moutures 1.0.2 et 1.0.1 sont affectées, ce n'est le cas ni pour la 1.0.0, ni pour la 0.9.8, lesquelles ne sont toutefois plus prises en charge depuis le 31 janvier 2015.

Utilisé par de nombreux sites Web et services en ligne pour mettre en œuvre les protocoles de chiffrement SSL (Secure Sockets Layer) et TLS (Transport Layer Security) destinés à sécuriser les échanges de données entre client et serveur, OpenSSL fait l'objet d'une surveillance accrue depuis l'épisode Heartbleed, survenu au printemps 2014 avec la faille CVE-2014-0160 qui permettait l'interception de données confidentielles.

La Core Infrastructure Initiative à la manœuvre

Les travaux menés en collaboration avec la Core Infrastructure Initiative – qui fédère de grands acteurs de la sphère IT autour de la fondation Linux – ont permis d'accélérer la diffusion de correctifs… dont certains colmatant des brèches sévères, selon ITespresso.

L'une d'entre elles, résorbée au mois de janvier, rendait possible le déchiffrement et la modification du trafic Web par une attaque de type « man-in-the-middle ». Une autre corrigée dans le même temps autorisait la prise en main, à distance, des applications serveur ou client instrumentant la couche de chiffrement du protocole UDP OpenSSL DTLS (Data Transport Layer Security) – offrant souvent des fonctionnalités de visioconférence.

Plus récemment, l'équipe OpenSSL avait éliminé une faille (CVE-2015-0204) utilisable pour affaiblir les clés de chiffrement.

A lire aussi :

Heartbleed : un an après, la faille est tombée dans l'oubli
Heartbleed : Google, Facebook, Microsoft financent les projets Open Source clés

Crédit photo : Maksim Kabakou / Shutterstock