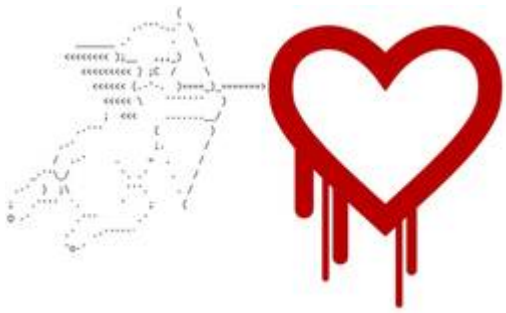
Alerte HeartBleed Acte II – Nom de code Cupid



Alerte HeartBleed Acte II – Nom de code Cupid

Cupid, nouvel exploit qui utilise la Heartbleed, ébranle les connexions Wi-Fi.

Pour l'instant, à l'état de preuve de concept, cette faille n'est sans doute que le premier écho du coup de tonnerre qui a fait trembler le Net en avril dernier.

Alerte HeartBleed Acte II – Nom de code Cupid

Heartbleed, la faille qui a ébranlé le Net, frappe des routeurs Wi-Fi et Android.
Cupid, c'est le nouvel exploit qui utilise Heartbleed et ébranle les connexions Wi-Fi.
Pour l'instant, à l'état de preuve de concept, cette faille n'est sans doute que le premier écho du coup de tonnerre qui a fait trembler le Net en avril dernier.

Heartbleed, la faille OpenSSL qui a mis à mal la sécurité du Net au début du mois d'avril dernier, frappe à nouveau.
Cette fois, Luis Gengeia, chercheur en sécurité portugais de la société SysValue, a trouvé une application, plus restreinte de cet exploit, qui s'en prend à certains routeurs Wi-Fi. Baptisée Cupid, cette variante touche les réseaux sans fil qui utilise les méthodes d'authentification EAP reposant sur OpenSSL (EAP-TLS).

Cette faille permet de récupérer des données provenant des routeurs et même d'utiliser un routeur infecté pour soutirer

des données à un appareil Android (sous Jelly Bean 4.1.1), qui s'y connecterait. Les smartphones sous cette version de l'OS de Google sont particulièrement sensibles à la faille Heartbleed, des mises à jour sont à appliquer d'urgence si disponibles.
Grâce à cette nouvelle faille, l'attaquant peut utiliser Heartbleed pour obtenir une clé privée auprès du routeur ou du serveur d'authentification, dans le cas d'une entreprise, en faisant fi des mesures de sécurité habituelles. Il accède ensuite au réseau en toute tranquillité.
L'expert en sécurité, qui estime que sa découverte n'est pour l'instant qu'au stade de preuve de concept explique ne pas avoir réalisé assez de tests pour savoir combien de routeurs pourraient être concernés. Par ailleurs, il précise que seuls les périphériques qui sont à portée d'un routeur corrompu sont des cibles potentielles.

L'arrivée de Cupid, alors que le Net n'est pas encore remis de la première vague Heartbleed montre que la route est encore longue et que de nombreuses failles et attaques, tirant parti de cet exploit, pourraient être dévoilées dans les mois et années à venir.

Cet article vous à plu ? Laissez-nous un commentaire

(notre source d'encouragements et de progrès)

Références :

02/06/2014 : http://www.zdnet.fr/actualites/cupidon-un-nouveau-vecteur-d-attaque-pour-heartbleed-39801811.htm

02/06/2014 : http://www.01net.com/editorial/620792/heartbleed-la-faille-qui

-a-ebranle-le-web-frappe-les-routeurs-wi-fi/