Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERTA

Paris, le 02 novembre 2012
N° CERTA-2012-ACT-044

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTA-2012-ACT-044

1 Compromission de F5 BIG-IP

Le 11 juin 2012, le CERTA a publié un avis (CERTA-2012-AVI-313) concernant une vulnérabilité du produit *F5 BIG-IP*. La vulnérabilité exposée dans cet avis a également fait l'objet d'un article du bulletin d'actualité CERTA-2012-ACT-024 du 15 juin 2012. Le principe de la faille repose sur la présence d'une clé privée, commune à tous les équipements *F5 BIG-IP*, qui permet de se connecter à distance, via SSH, sur le compte *root* du matériel.

Le 12 juin 2012, des outils permettant d'exploiter automatiquement cette vulnérabilité étaient publiés sur l'Internet.

Le CERTA a récemment traité le cas d'une compromission d'un matériel *F5 BIG-IP*. L'analyse des journaux du boîtier a permis de mettre en évidence une connexion SSH illégitime sur le compte *root* du système, laissant supposer l'exploitation de la vulnérabilité mentionnée précédemment.

Les risques associés aux intrusions sur ce type de matériel sont :

- des rebonds vers des machines internes du réseau ;
- des attaques vers des machines à l'extérieur du réseau ;
- des attaques de type homme-au-milieu (*man-in-the-middle*) ;
- une modification de la configuration de l'équipement.

Le CERTA recommande aux administrateurs de *F5 BIG-IP* :

- d'appliquer rapidement les correctifs de sécurité pour ce produit ;
- de s'assurer que les journaux sont correctement configurés pour enregistrer les connexions au boîtier ;
- de chercher dans les journaux des traces d'éventuelle compromission (typiquement des connexions SSH illégitimes) ;
- de mettre en place un filtrage (au moins pour SSH) si la configuration réseau le permet.

Documentation

- Avis CERTA-2012-AVI-313 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2012-AVI-313/
- Bulletin d'actualité CERTA-2012-ACT-024 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2012-ACT-024/

2 Vérification des certificats SSL dans les applications client

Le 16 octobre 2012, lors de la conférence ACM CCS 2012, il a été présenté qu'une attaque de type homme-au-milieu (*man-in-the-middle*) est réalisable dans certaines applications client utilisant SSL. L'étude recense plusieurs catégories d'applications vulnérables comme par exemple : des clients de messagerie instantanée, des applications de paiement et des applications mobiles. Les navigateurs Web ne sont pas concernés par cette étude.

Pour empêcher les attaques de type homme-au-milieu lors d'une connexion SSL, le client doit vérifier un certain nombre de conditions comme par exemple :

- le certificat du serveur a été émis par une authorité reconnue (vérifier la chaîne de confiance) ;
- la date d'expiration du certificat n'est pas atteinte ;
- le certificat n'a pas été révoqué ;
- le nom de domaine du serveur correspond bien au nom de domaine présent dans le certificat.

Cette étude montre plusieurs exemples d'applications client qui ne suivent pas toutes ces étapes pour verifier le certificat SSL du serveur. En général, la vulnérabilité vient d'une mauvaise utilisation de la bibliothèque SSL comme OpenSSL, GnuTLS, BouncyCastle, JSSE, cURL, NSS et bien d'autres.

Un exemple accessible est celui de la bibliothèque cURL. Pour vérifier la chaîne de confiance et le nom de domaine, le développeur doit définir deux paramètres ayant des noms similaires mais des types différents. En effet, le premier paramètre est un booléen et le deuxième paramètre un entier : une confusion de type est assez fréquente pour le deuxième paramètre et désactive la vérification du nom de domaine.

Le constat est que les mauvaises utilisations des bibliothèques SSL ne sont pas des cas isolés et sont mêmes répandues. Le CERTA recommande aux utilisateurs d'être vigilants avec les clients SSL qu'ils utilisent, particulièrement sur des réseaux qui ne sont pas de confiance. Le CERTA conseille aux développeurs qui utilisent le protocole SSL dans leurs applications de correctement utiliser les bibliothèques SSL en respectant les consignes de la documentation.

Documentation

- Article « The Most Dangerous Code in the World: Validating SSL Certificates in Non-Browser Software » : https://crypto.stanford.edu/ dabo/pubs/abstracts/ssl-client-bugs.html

3 Les sites de téléchargement de logiciels

Certains sites Web à large audience proposent un catalogue très complet de logiciels à télécharger. De nombreux utilitaires tels que des programmes de compression, des navigateurs ou encore des antivirus peuvent y être téléchargés. Ces sites sont souvent privilégiés pour l'installation de ces logiciels du fait de leur simplicité et parce qu'ils sont souvent dans les premiers résultats des moteurs de recherche. Afin de rentabiliser l'hébergement, ces sites de téléchargement ajoutent parfois des programmes publicitaires, des barres d'outils ou modifient la page d'accueil voire le moteur de recherche par défaut dans les navigateurs.

Récemment, certains utilisateurs ont vu apparaître des publicités intempestives suite à l'installation d'un logiciel issu de l'un de ces sites. En réalisant une analyse antivirale sur le programme en question, il est apparu qu'un module destiné à afficher de la publicité ciblée avait été ajouté à l'installateur. La présence de logiciels additionnels pose plusieurs problèmes. Tout d'abord, une partie du code exécuté n'est pas maitrisée par l'éditeur original du logiciel installé. En effet, dans le meilleur des cas il s'agit d'une publicité intempestive, mais il arrive parfois qu'un code malveillant infecte le poste sur lequel il est exécuté. Ensuite, l'installation de barres d'outils implique la plupart du temps l'acceptation de conditions d'utilisation telles que, par exemple, la possibilité d'utiliser les données personnelles collectées à des fins commerciales.

Au-delà de la confiance que l'on peut accorder aux sites Web de téléchargement, chaque intermédiaire entre l'éditeur original du logiciel et l'utilisateur final peut potentiellement être compromis. L'ajout d'un maillon dans la chaîne de distribution constitue donc un risque supplémentaire. Enfin, la plateforme d'hébergement de logiciels multiples introduit un délai pour diffuser les nouvelles versions d'un logiciel. Les mises à jour sont donc disponibles plus tardivement et exposent les postes de travail plus longtemps aux vulnérabilités. Le CERTA recommande donc de toujours utiliser le site Web officiel du logiciel désiré. De plus, lorsque cela est possible, il est recommandé de vérifier la signature numérique du programme.

4 Rappel des avis émis

Dans la période du 26 octobre au 01 novembre 2012, le CERTA a émis les publications suivantes :

- CERTA-2012-AVI-604 : Vulnérabilité dans des produits HP, 3COM et H3C
- CERTA-2012-AVI-605 : Vulnérabilité dans Xen
- CERTA-2012-AVI-606 : Multiples vulnérabilités dans IBM InfoSphere
- CERTA-2012-AVI-607 : Multiples vulnérabilités dans IBM WebSphere MQ
- CERTA-2012-AVI-608 : Vulnérabilité dans Exim DKIM
- CERTA-2012-AVI-609 : Multiples vulnérabilités dans les produits Mozilla
- CERTA-2012-AVI-610 : Multiples vulnérabilités dans Request Tracker
- CERTA-2012-AVI-611 : Vulnérabilité dans Tiki wiki CMS groupware
- CERTA-2012-AVI-612 : Vulnérabilités dans phpMyAdmin
- CERTA-2012-AVI-613 : Vulnérabilité dans EMC Avamar

Gestion détaillée du document

02 novembre 2012 version initiale.