Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERT-FR

Paris, le 11 avril 2014
N° CERTFR-2014-ACT-015

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2014-ACT-015

1 - Heartbleed : vulnérabilité OpenSSL

Le protocole SSL/TLS est utilisé pour assurer la sécurisation des échanges sur Internet (chiffrement des communications, authentification, etc.). Le 7 avril 2014, une vulnérabilité a été publiée concernant certaines versions de OpenSSL qui est une implémentation libre et massivement utilisée de ce protocole. La vulnérabilité identifiée permet à un attaquant de pouvoir lire arbitrairement des données présentes dans la mémoire d'un système ciblé. Cela a par exemple comme conséquence, dans le cas de serveurs web, de pouvoir accéder à des données secrètes comme des mots de passe.

OpenSSL, *heartbeat* et la vulnérabilité *heartbleed*

La vulnérabilité identifiée (nommée *heartbleed*) se situe au niveau de l'implémentation de l'extension *heartbeat* par OpenSSL. Cette extension, présente depuis la version 1.0.1 d'OpenSSL, permet de maintenir une connexion ouverte entre un client et un serveur. La fonctionnalité d'*heartbeat* est définie de la façon suivante :

- le client envoie une requête de type *heartbeat* au serveur contenant notamment une charge utile (définie par le client) et la taille de cette charge utile ;
- le serveur répond en renvoyant un paquet contenant une charge utile correspondant à celle envoyée par le client.

Dans les versions vulnérables d'OpenSSL, le serveur ne prend en compte que la taille indiquée par le client et ne vérifie pas si elle est cohérente avec la taille effective de la charge utile qu'il a envoyée, ni même si une charge utile est réellement envoyée par le client. Autrement dit, si la taille indiquée est supérieure à celle de la charge utile effective, alors le serveur renverra aléatoirement des données présentes dans la mémoire vive du système. Les données présentes dans la mémoire vive peuvent être de différentes natures. Mais dans le cas d'un serveur web, où l'activité principale est le traitement de requêtes d'utilisateurs, les données renvoyées sont en général le contenu de ces requêtes (avant ou après traitement). Il peut donc s'agir :

- de contenu de pages web ;
- des données d'authentification transmises par les clients (et donc principalement des couples noms d'utilisateur/mots de passe ou des cookies) ;
- du code source (par exemple PHP) en cours d'évaluation ;
- potentiellement des clés de chiffrement utilisées par le serveur ;
- etc.

L'exploitation de cette vulnérabilité par un attaquant peut alors potentiellement rendre accessible tout le contenu normalement chiffré d'une communication effectuée avec OpenSSL. De plus, cette vulnérabilité étant publique, de nombreuses personnes tentent activement de l'exploiter, augmentant ainsi le risque de fuites de données sensibles. En outre, la vulnérabilité affecte aussi le client OpenSSL. Ainsi, les clients utilisant OpenSSL peuvent être également vulnérables en cas de connexions à un serveur malveillant.

Diagnostic

Une activité de type *heartbeat* étant par définition légitime, il est très difficile de savoir *a posteriori* si les données d'un serveur ont pu être compromises par une exploitation de la vulnérabilité : aucune journalisation au niveau applicatif ne peut être effectuée concernant ce type d'échanges. Néanmoins, il est possible de savoir si un serveur est vulnérable en vérifiant dans un premier temps si l'extension *heartbeat* est disponible, puis en vérifiant si la version d'OpenSSL présente est vulnérable.

Pour vérifier si l'extension *heartbeat* est disponible sur un serveur donné, il faut exécuter la commande suivante :

```
openssl s_client -connect <adresse du serveur>:<port> -tlsextdebug | grep "TLS server extension"
```

Si le retour de cette commande contient la ligne suivante alors l'extension *hearbeat* est disponible :

```
TLS server extension "heartbeat" (id=15), len=1
```

Le cas écheant, il faut alors vérifier si la version d'OpenSSL présente est impactée par la vulnérabilité : les versions vulnérables vont de la 1.0.1 à la 1.0.1f, ainsi que la 1.0.2-beta1 (les versions antérieures à 1.0.1 ne sont sont pas impactées). Il convient de noter également que de nombreux produits peuvent embarquer leur propre version d'OpenSSL sans utiliser celle potentiellement déjà en place sur le système. Il convient alors d'effectuer le diagnostic pour chacun des produits embarquant potentiellement sa propre version d'OpenSSL.

Pour information, les principaux services qui peuvent être impactés sont :

- HTTPS,
- SMTP sur SSL (ou avec STARTTLS),
- IMAP sur SSL,
- POP3 sur SSL,
- passerelle VPN avec SSL.

Recommandations

Le CERT-FR recommande de vérifier si une version d'OpenSSL vulnérable est présente sur les serveurs exposés sur Internet et le cas échéant de mettre à jour OpenSSL vers la version 1.0.1g corrigeant cette vulnérabilité.

Les mises à jour doivent s'appliquer aussi bien aux systèmes d'exploitation qu'aux équipements réseau ou aux applications embarquant OpenSSL. De nombreux éditeurs ont d'ores et déjà publié des correctifs :

- Ubuntu :
  http://www.ubuntu.com/usn/usn-2165-1/
- Debian :
  http://www.debian.org/security/2014/dsa-2896
- RedHat :
  https://rhn.redhat.com/errata/RHSA-2014-0376.html
- CentOS :
  http://lists.centos.org/pipermail/centos-announce/2014-April/020249.html
- Juniper :
  http://kb.juniper.net/InfoCenter/index?page=contentid=JSA10623cat=SIRT_1actp=LIST
- Cisco :
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140409-heartbleed
- OpenVPN :
  https://openvpn.net/index.php/access-server/download-openvpn-as-sw/532-release-notes-v200.html

Une fois la mise à jour appliquée et les différents produits mis à jour, il est nécessaire de redémarrer les services utilisant OpenSSL afin de charger la nouvelle version. Comme il est quasiment impossible de savoir si des données ont été compromises, le CERT-FR recommande également, une fois la mise à jour effectuée, de réinitialiser toutes les sessions en cours et de communiquer auprès des utilisateurs s'étant connectés sur les serveurs impactés pour les inviter à procéder à un changement de mot de passe. Enfin, en cas de suspicion de compromission des clés de chiffrement, le CERT-FR recommande de révoquer les certificats correspondants et de régénérer les clés.

En complément, le CERT-FR indique que des signatures pour les systèmes de détection d'intrusion Snort et Suricata ont été proposées publiquement sur Internet :

- règles Suricata (par Inliniac) :
  http://blog.inliniac.net/2014/04/08/detecting-openssl-heartbleed-with-suricata/

– règles Snort (par FOX-IT) :
http://blog.fox-it.com/2014/04/08/openssl-heartbleed-bug-live-blog/

Documentation

– Bulletin de sécurité OpenSSL du 7 avril 2014 :
https://www.openssl.org/news/secadv_20140407.txt
– Présentation de la vulnérabilité *heartbleed* :
http://heartbleed.com/
– Avis du CERT-FR :
http://cert.ssi.gouv.fr/site/CERTFR-2014-AVI-156/index.html
– Référence CVE (CVE-2014-0160) :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160

2 - La sécurité des systèmes d'information et le facteur humain

Les politiques de sécurité des systèmes d'information s'appuient généralement sur des solutions techniques plus ou moins complexes. Cependant, pour être réellement efficaces, elles doivent impérativement prendre en compte le facteur humain.

Les incidents traités par le CERT-FR confirment que les employés participent très souvent, par leur comportement, à garantir l'intégrité d'un système d'information ou à le mettre en péril.

Les utilisateurs, même s'ils n'en ont pas toujours conscience, sont très fréquemment placés en première ligne lors d'une tentative de compromission. Les attaquants essaient par de nombreux moyens de les convaincre d'exécuter un programme malveillant, de cliquer sur un lien illégitime ou plus simplement de communiquer des informations sensibles. Des moyens techniques efficaces existent pour protéger le système d'information lorsque l'un de ses utilisateurs adopte, souvent sans s'en rendre compte, un comportement inadapté. Cependant, ils restent perfectibles et l'échec ou la réussite de l'attaque dépendra souvent du comportement de l'employé.

Il est alors clair que la sécurité d'une infrastructure ne peut reposer uniquement sur des solutions techniques et que l'utilisateur doit jouer un rôle prépondérant. Cependant, ce dernier ne sera en mesure de jouer son rôle que s'il a été convenablement sensibilisé et formé. Une formation adaptée, élément fondamental de la politique de sécurité, permettra aux membres de l'organisation d'acquérir les connaissances techniques nécessaires, d'adopter de bonnes pratiques et de prendre conscience de leur rôle dans la protection du réseau de l'entreprise.

Ils doivent être informés des risques liés à l'utilisation des applications du quotidien (messagerie, navigateur Internet, etc.) et des modes opératoires classiques des attaques informatiques (programmes néfastes, sites Internet malveillants, ingénierie sociale, etc.). Conscients des dangers que certaines attitudes peuvent faire peser sur le système d'information, ils participent à réduire les risques de compromission.

Dans la pratique, le CERT-FR constate que les employés savent rarement que la consultation d'une page web ou un simple clic sur un programme peut mettre à mal l'ensemble du système d'information d'une société. L'utilisateur doit également pouvoir utiliser des procédures simples pour signaler aux correspondants informatiques les incidents ou anomalies constatés. Correctement formé, il peut participer à la détection des premiers signes d'une attaque informatique. Plus un incident est détecté rapidement plus il est simple d'y mettre un terme. La sécurité d'un système informatique passe impérativement par la sensibilisation de l'utilisateur. Le facteur humain pourra alors être perçu comme un atout pour la sécurité du parc et non, comme certains le décrivent, un "maillon faible".

Documentation

– Guide d'hygiène informatique (règles 39 et 37) :
http://www.ssi.gouv.fr/IMG/pdf/guide_hygiene_informatique_anssi.pdf
– Bulletin d'actualité CERTFR-2014-ACT-008 :
http://www.cert.ssi.gouv.fr/site/CERTFR-2014-ACT-008/index.html

3 - Mise à jour mensuelle Microsoft

Lors de sa dernière mise à jour mensuelle, Microsoft a publié quatre bulletins de sécurité, dont deux sont considérés comme critiques :

- MS14-017 (critique) qui concerne Microsoft Office et corrige notamment la faille CVE-2014-1761 dans Word ;
- MS14-018 (critique) qui concerne Internet Explorer et corrige six vulnérabilités liées à des corruptions mémoire ;
- MS14-019 (important) qui concerne le traitement des fichiers .bat et .cmd distants ;
- MS14-020 (important) qui concerne Microsoft Publisher.

La faille CVE-2014-1761 est une vulnérabilité dans le traitement par Word de certains fichiers RTF mal formés. Elle avait été exploitée dans des attaques ciblées avant que le correctif ne soit disponible et avait donné lieu à l'alerte CERTFR-2014-ALE-002, désormais close. Les six failles référencées dans le bulletin MS14-018 affectent plusieurs versions d'Internet Explorer entre la 6 et la 11 et seraient susceptibles, en l'absence du correctif, de permettre une exécution de code arbitraire à distance. A ce stade, il n'y a pas de code d'exploitation public connu. Il est à noter que les correctifs du mois d'Avril pour Windows XP et Office 2003 sont les derniers disponibles. En effet, ces logiciels ne sont plus supportés par Microsoft et ne seront plus mis à jour. Comme cela a déjà été mentionné dans les précédents bulletins d'actualité, le CERT-FR recommande donc de migrer vers des systèmes supportés par leurs éditeurs et bénéficiant de mises à jour de sécurité.

Documentation

- http://www.cert.ssi.gouv.fr/site/CERTFR-2014-AVI-157/index.html
- http://www.cert.ssi.gouv.fr/site/CERTFR-2014-AVI-158/index.html
- http://www.cert.ssi.gouv.fr/site/CERTFR-2014-AVI-159/index.html
- http://www.cert.ssi.gouv.fr/site/CERTFR-2014-AVI-160/index.html
- http://www.cert.ssi.gouv.fr/site/CERTFR-2014-ALE-002/index.html

4 - Rappel des avis émis

Dans la période du 04 au 10 avril 2014, le CERT-FR a émis les publications suivantes :

- CERTFR-2014-ALE-003 : Vulnérabilité dans OpenSSL
- CERTFR-2014-AVI-156 : Vulnérabilité dans OpenSSL
- CERTFR-2014-AVI-157 : Multiples vulnérabilités dans Microsoft Office
- CERTFR-2014-AVI-158 : Multiples vulnérabilités dans Microsoft Internet Explorer
- CERTFR-2014-AVI-159 : Vulnérabilité dans Microsoft Windows
- CERTFR-2014-AVI-160 : Vulnérabilité dans Microsoft Publisher
- CERTFR-2014-AVI-161 : Vulnérabilité dans plusieurs produits Cisco
- CERTFR-2014-AVI-162 : Vulnérabilité dans plusieurs produits Juniper
- CERTFR-2014-AVI-163 : Multiples vulnérabilités dans Adobe Flash
- CERTFR-2014-AVI-164 : Multiples vulnérabilités dans Google Chrome
- CERTFR-2014-AVI-165 : Vulnérabilité dans Citrix VDI-in-a-Box
- CERTFR-2014-AVI-166 : Multiples vulnérabilités dans WordPress
- CERTFR-2014-AVI-167 : Vulnérabilité dans OpenVPN Access Server
- CERTFR-2014-AVI-168 : Multiples vulnérabilités dans Cisco ASA
- CERTFR-2014-AVI-169 : Vulnérabilité dans plusieurs produits Blue Coat
- CERTFR-2014-AVI-170 : Vulnérabilité dans WireShark
- CERTFR-2014-AVI-171 : Vulnérabilité dans Juniper Junos
- CERTFR-2014-AVI-172 : Vulnérabilité dans Juniper Junos
- CERTFR-2014-AVI-173 : Vulnérabilité dans Juniper Junos
- CERTFR-2014-AVI-174 : Vulnérabilité dans Juniper Junos
- CERTFR-2014-AVI-175 : Vulnérabilité dans Juniper Junos

Durant la même période, les publications suivantes ont été mises à jour :

- CERTFR-2014-ALE-002-001 : Vulnérabilité dans Microsoft Word (fermeture de l'alerte, suite à la diffusion du correctif par l'éditeur.)

Gestion détaillée du document

11 avril 2014 version initiale.

Conditions d'utilisation de ce document :	`http://cert.ssi.gouv.fr/cert-fr/apropos.html`
Dernière version de ce document :	`http://cert.ssi.gouv.fr/site/CERTFR-2014-ACT-015`