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 08 avril 2014
N° CERTFR-2014-AVI-156

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Vulnérabilité dans OpenSSL

Gestion du document

Référence	CERTFR-2014-AVI-156
Titre	Vulnérabilité dans OpenSSL
Date de la première version	08 avril 2014
Date de la dernière version	–
Source(s)	Bulletin de sécurité OpenSSL du 07 avril 2014
Pièce(s) jointe(s)	Aucune

TAB. 1 – *Gestion du document*

Une gestion de version détaillée se trouve à la fin de ce document.

1 - Risque(s)

- contournement de la politique de sécurité
- atteinte à la confidentialité des données

2 - Systèmes affectés

- OpenSSL 1.0.1, version 1.0.1f et antérieures
- OpenSSL 1.0.2-beta1

3 - Résumé

Une vulnérabilité a été corrigée dans *OpenSSL*. Elle permet à un attaquant de provoquer un contournement de la politique de sécurité et une atteinte à la confidentialité des données.

4 - Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

5 - Documentation

- Bulletin de sécurité OpenSSL du 07 avril 2014
  https://www.openssl.org/news/secadv_20140407.txt
- Description de la vulnérabilité
  http://heartbleed.com/
- Référence CVE CVE-2014-0160
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160
- Bulletin d'alerte du CERT-FR
  http://www.cert.ssi.gouv.fr/site/CERTFR-2014-ALE-003/
- Bulletin de sécurité Red Hat RHSA-2014:0376-1
  https://rhn.redhat.com/errata/RHSA-2014-0376.html
- Bulletin d'alerte Fedora FEDORA-2014-4910
  https://lwn.net/Articles/594066/
- Bulletin de sécurité opensuse SUSE-SA:2014:002
  http://lists.opensuse.org/opensuse-security-announce/2014-04/msg00005.html
- Bulletin d'alerte Debian DSA-2896-1
  http://www.debian.org/security/2014/dsa-2896
- Bulletin de sécurité FreeBSD FreeBSD-SA-14:06.openssl
  http://www.freebsd.org/security/advisories/FreeBSD-SA-14:06.openssl.asc

Gestion détaillée du document

08 avril 2014 version initiale.