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 30 juillet 2014
N° CERTFR-2014-ALE-003-002

Affaire suivie par :
CERT-FR

BULLETIN D'ALERTE DU CERT-FR

Objet : Vulnérabilité dans OpenSSL

Gestion du document

Référence	CERTFR-2014-ALE-003-002
Titre	Vulnérabilité dans OpenSSL
Date de la première version	08 avril 2014
Date de la dernière version	30 juillet 2014
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 découverte 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
- Référence CVE CVE-2014-0160
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160
- Description de la vulnérabilité
  http://heartbleed.com/
- Avis du CERT-FR
  http://www.cert.ssi.gouv.fr/site/CERTFR-2014-AVI-156/
- Bulletin d'actualité CERTFR-2014-ACT-015
  http://www.cert.ssi.gouv.fr/site/CERTFR-2014-ACT-015/

Gestion détaillée du document

08 avril 2014 version initiale ;
15 avril 2014 mise à jour de l'alerte ;
30 juillet 2014 fermeture de l'alerte.