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 12 juin 2015
N° CERTFR-2015-AVI-257

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Multiples vulnérabilités dans OpenSSL

Gestion du document

Référence	CERTFR-2015-AVI-257
Titre	Multiples vulnérabilités dans OpenSSL
Date de la première version	12 juin 2015
Date de la dernière version	–
Source(s)	Bulletin de sécurité OpenSSL secadv$_2$0150611du11$juin$2015
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)

- déni de service à distance
- atteinte à la confidentialité des données

2 - Systèmes affectés

- OpenSSL 1.0.2
- OpenSSL 1.0.1
- OpenSSL 1.0.0d et antérieures
- OpenSSL 0.9.8r et antérieures
- OpenSSL 1.0.0

3 - Résumé

De multiples vulnérabilités ont été corrigées dans *OpenSSL*. Elles permettent à un attaquant de provoquer un déni de service à distance 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 secadv_20150611 du 11 juin 2015
  https://www.openssl.org/news/secadv_20150611.txt
- Référence CVE CVE-2015-4000
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4000
- Référence CVE CVE-2015-1788
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1788
- Référence CVE CVE-2015-1789
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1789
- Référence CVE CVE-2015-1790
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1790
- Référence CVE CVE-2015-1792
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1792
- Référence CVE CVE-2015-1791
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1791
- Référence CVE CVE-2014-8176
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8176

Gestion détaillée du document

12 juin 2015 version initiale.