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 04 décembre 2015
N° CERTFR-2015-AVI-517

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Multiples vulnérabilités dans OpenSSL

Gestion du document

Référence	CERTFR-2015-AVI-517
Titre	Multiples vulnérabilités dans OpenSSL
Date de la première version	04 décembre 2015
Date de la dernière version	–
Source(s)	Bulletin de sécurité OpenSSL du 03 décembre 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 l'intégrité des données
- atteinte à la confidentialité des données

2 - Systèmes affectés

- OpenSSL 1.0.2 versions antérieures à 1.0.2e
- OpenSSL 1.0.1 versions antérieures à 1.0.1q
- OpenSSL 1.0.0 versions antérieures à 1.0.0t
- OpenSSL 0.9.8 versions antérieures à 0.9.8zh

3 - Résumé

De multiples vulnérabilités ont été corrigées dans *OpenSSL*. Elles permettent à un attaquant de provoquer un déni de service à distance, une atteinte à l'intégrité des données 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 03 décembre 2015
  https://openssl.org/news/secadv/20151203.txt
- Référence CVE CVE-2015-3193
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3193
- Référence CVE CVE-2015-3194
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3194
- Référence CVE CVE-2015-3195
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3195
- Référence CVE CVE-2015-3196
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3196

Gestion détaillée du document

04 décembre 2015 version initiale.