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 29 janvier 2016
N° CERTFR-2016-AVI-041

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Multiples vulnérabilités dans OpenSSL

Gestion du document

Référence	CERTFR-2016-AVI-041
Titre	Multiples vulnérabilités dans OpenSSL
Date de la première version	29 janvier 2016
Date de la dernière version	–
Source(s)	Bulletin de sécurité OpenSSL 20160128 du 28 janvier 2016
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 l'intégrité des données
- atteinte à la confidentialité des données

2 - Systèmes affectés

- OpenSSL versions 1.0.2x antérieures à 1.0.2f
- OpenSSL versions antérieures à 1.0.1r

3 - Résumé

De multiples vulnérabilités ont été corrigées dans *OpenSSL*. Elles permettent à un attaquant de provoquer un contournement de la politique de sécurité, 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 20160128 du 28 janvier 2016
  https://www.openssl.org/news/secadv/20160128.txt
- Référence CVE CVE-2016-0701
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0701
- Référence CVE CVE-2015-3197
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3197

Gestion détaillée du document

29 janvier 2016 version initiale.