Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERTA

Paris, le 30 mai 2012
N° CERTA-2012-AVI-299

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans PyCrypto

Gestion du document

Référence	CERTA-2012-AVI-299
Titre	Vulnérabilité dans PyCrypto
Date de la première version	30 mai 2012
Date de la dernière version	–
Source(s)	Journal de modifications de version de PyCrypto
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

Atteinte à la confidentialité des données.

2 Systèmes affectés

PyCrypto versions 2.5 et antérieures.

3 Résumé

Une vulnérabilité a été corrigée dans PyCrypto. Une erreur dans la génération des clés ElGamal permet à un attaquant de reduire grandement l'espace de clés dans le cas d'une attaque par recherche exhaustive.

4 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation). La version 2.6 de PyCrypto corrige le problème. Les clés ElGamal générées avec une version antérieure devront être regénérées.

5 Documentation

- Journal de modifications de version de PyCrypto :
  https://github.com/dlitz/pycrypto/blob/373ea760f21701b162e8c4912a66928ee30d401a/ChangeLog
- Référence CVE CVE-2012-2417 :
  http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-2417

Gestion détaillée du document

30 mai 2012 version initiale.