



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 31 août 2000  
N° CERTA-2000-AVI-040

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité sous PGP 5.5.x à 6.5.3

---

Conditions d'utilisation de ce document : <http://www.certa.ssi.gouv.fr/certa/apropos.html>  
Dernière version de ce document : <http://www.certa.ssi.gouv.fr/site/CERTA-2000-AVI-040>

---

### Gestion du document

Référence	CERTA-2000-AVI-040
Titre	Vulnérabilité sous PGP 5.5.x à 6.5.3
Date de la première version	31 août 2000
Date de la dernière version	–
Source(s)	Avis CA-2000-18 du CERT/CC
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

- Compromission des informations ;
- Perte de confidentialité des données.

## 2 Systèmes affectés

PGP versions 5.5.x à 6.5.3

## 3 Résumé

La possibilité d'ajouter une clé supplémentaire de déchiffrement (ADK : Additional Decryption Keys) dans le certificat d'une clé publique a été introduite avec la version 5.5 de PGP

Le chiffrement des données par les versions 5.5.x jusqu'à 6.5.3 de PGP, et utilisant un certificat modifié, génère un texte chiffré avec la clé ADK.

L'utilisateur malveillant qui a modifié un certificat peut, sous certaines conditions, obtenir le texte clair correspondant.

PGP ne détecte pas ce type de certificat modifié du fait d'une erreur dans son implémentation.

## 4 Description

La fonctionnalité ADK permet d'ajouter une seconde clé de chiffrement dans le certificat de la clé publique d'un utilisateur.

Toutes les données chiffrées avec la clé primaire sont aussi chiffrées avec la seconde clé (ADK). Cette fonctionnalité permet, par exemple, de rajouter systématiquement dans les certificats des différentes personnes d'une entreprise, la clé de l'entreprise.

La fonctionnalité ADK est prévue uniquement dans le cas où l'utilisateur autorise l'ajout d'une clé ADK dans son certificat. Malheureusement, du fait d'une mauvaise implémentation dans la vérification du certificat, un utilisateur malveillant peut ajouter sans l'accord de l'utilisateur une clé ADK dans son certificat.

Plusieurs conditions doivent être réunies afin d'exploiter cette vulnérabilité :

- L'expéditeur doit avoir une version de PGP vulnérable (GnuPGP-1.0.1 n'est pas vulnérable) ;
- L'expéditeur doit chiffrer avec un certificat modifié ;
- L'expéditeur doit valider la boîte de dialogue lui indiquant la présence d'une clé ADK ;
- L'expéditeur doit posséder le certificat modifié dans son fichier de clés publiques local ;
- Le certificat modifié doit être signé par une autorité dans laquelle l'expéditeur a confiance ;
- Les données chiffrées doivent être interceptées par l'utilisateur malveillant.

Comme le propriétaire de la clé ADK est clairement cité comme destinataire du message chiffré, il est de ce fait facilement identifiable.

## 5 Solution

Correctif PGP :

<http://www.pgp.com/other/advisories/adk-product-info-center.asp>

Une nouvelle version de PGP (6.5.8) corrigeant cette vulnérabilité est disponible depuis le 25 Août 2000 :

<http://www.pgpi.org>

## 6 Documentation

Avis du CERT/CC :

<http://www.cert.org/advisories/CA-2000-18.html>

Avis PGP :

<http://www.pgp.com/other/advisories/adk.asp>

Rapport de Ralf Sendereck sur cette vulnérabilité :

<http://sendereck.de/security/key-experiments.html>

## Gestion détaillée du document

**31 août 2000** version initiale.