Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 12 août 2005
N° CERTA-2005-AVI-312

**Affaire suivie par :**
CERTA

# AVIS DU CERTA

## Objet : Vulnérabilité dans l'implémentation de IPsec sur HP Tru64



## Gestion du document

| | |
|---|---|
| Référence | CERTA-2005-AVI-312 |
| Titre | Vulnérabilité dans l'implémentation de IPsec sur HP Tru64 |
| Date de la première version | 12 août 2005 |
| Date de la dernière version | – |
| Source(s) | Bulletin de sécurité HP SSRT5957 du 9 août 2005 |
| 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

- HP Tru64 UNIX 5.1B-3;
- HP Tru64 UNIX 5.1B-2/PK4.

## 3 Résumé

Une vulnérabilité dans l'implémentation de IPsec sur HP Tru64 permet à un utilisateur distant mal intentionné de porter atteinte à la confidentialité de données.

## 4 Description

Une erreur dans la mise en œuvre de l'ESP (Encapsulating Security Payload) en mode tunnel de IPsec sur les systèmes HP Tru64 permet à un utilisateur distant mal intentionné de porter atteinte à la confidentialité des données en modifiant malicieusement le paquet cible afin d'obtenir un message d'erreur ICMP (Internet Control Message Protocol) contenant une partie du contenu du paquet initial en clair.

Remarque: L'`IPsec` en mode tunnel `ESP` doit être configuré sans protection d'intégrité pour que l'utilisation de cette vulnérabilité soit exploitable.

# 5 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

# 6 Documentation

- Bulletin de sécurité HP HP SSRT5957 du 9 août 2005 :
  http://itrc.hp.com/service/cki/docDisplay.do?docId=HPSBTU01217
- Référence CVE CAN-2005-0039 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0039

# Gestion détaillée du document

**12 août 2005** version initiale.