

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans divers produits F-Secure

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-2005-AVI-442>

Gestion du document

Référence	CERTA-2005-AVI-442
Titre	Vulnérabilité dans divers produits F-Secure
Date de la première version	08 novembre 2005
Date de la dernière version	–
Source(s)	Bulletin de sécurité FSC-2005-3 de F-Secure du 07 novembre 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

Elévation de privilèges.

2 Systèmes affectés

- F-Secure Anti-Virus Internet Gatekeeper pour Linux versions antérieures à 2.15.484 ;
- F-Secure Anti-Virus Linux Gateway versions antérieures à 2.16.

3 Description

L'installation des produits F-Secure Anti-Virus Internet Gatekeeper pour Linux et F-Secure Anti-Virus Linux Gateway entraîne la création de scripts CGI ayant des droits en exécution pour tous avec le paramètre SUID activé. Un utilisateur local peut obtenir les droits de l'administrateur en utilisant ces scripts.

4 Contournement provisoire

Modifier les paramètres des scripts à l'aide des commandes ci-dessous.

- Pour F-Secure Anti-Virus Internet Gatekeeper pour Linux:
chmod -s /opt/f-secure/fsigk/cgi/*suid.cgi
- Pour F-Secure Anti-Virus Linux Gateway:
chmod -s /home/virusgw/cgi/*suid.cgi

5 Solution

Appliquer le correctif tel qu'indiqué dans le bulletin de sécurité F-Secure (voir Documentation).

6 Documentation

Bulletin de sécurité FSC-2005-3 de F-Secure du 07 novembre 2005 :
<http://www.f-secure.com/security/fsc-2005-3.shtml>

Gestion détaillée du document

08 novembre 2005 version initiale.