

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans Flex

---

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-2006-AVI-110>

---

### Gestion du document

Référence	CERTA-2006-AVI-110-001
Titre	Vulnérabilité dans Flex
Date de la première version	14 mars 2006
Date de la dernière version	28 mars 2006
Source(s)	Liste des mises à jour Freshmeat du 22 février 2006
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

Exécution de code arbitraire à distance.

## 2 Systèmes affectés

Flex versions 2.5.52 et antérieures.

## 3 Résumé

Une vulnérabilité dans Flex permet à un utilisateur mal intentionné d'exécuter du code arbitraire à distance.

## 4 Description

Flex est un outil libre permettant la création d'analyseurs lexicaux (*parsers*) en langage C. Il est utilisé dans de nombreux autres logiciels libres pour y faciliter la création d'analyseurs lexicaux.

Une erreur dans le fichier *flex.skl* permet à un utilisateur mal intentionné d'exécuter du code arbitraire à distance par le biais d'un analyseur lexical créé avec Flex et mettant en œuvre une grammaire comportant des règles utilisant la directive *REJECT* ou de type *trailing context*.

## 5 Solution

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

## 6 Documentation

- Liste des mises à jour Freshmeat du 22 février 2006 :  
<http://archives.neohapsis.com/archives/apps/freshmeat/2006-02/0022.html>
- Bulletin de sécurité Gentoo GLSA-200603-07 du 14 mars 2006 :  
<http://www.gentoo.org/security/en/glsa/glsa-200603-07.xml>
- Bulletin de sécurité Ubuntu USN-260-1 du 14 mars 2006 :  
<http://www.ubuntulinux.org/usn/usn-260-1>
- Bulletin de sécurité Debian DSA-1020 du 28 mars 2006 :  
<http://www.debian.org/security/2006/dsa-1020>
- Référence CVE CAN-2006-0459 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2006-0459>

## Gestion détaillée du document

**14 mars 2006** version initiale.

**28 mars 2006** ajout de la référence au bulletin de sécurité Debian.