

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités dans les produits Mozilla

---

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-055>

---

### Gestion du document

Référence	CERTA-2006-AVI-055-001
Titre	Multiples vulnérabilités dans les produits Mozilla
Date de la première version	03 février 2006
Date de la dernière version	07 février 2006
Source(s)	Bulletins de sécurité Mozilla
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 ;
- contournement de la politique de sécurité ;
- atteinte à la confidentialité des données.

## 2 Systèmes affectés

- Mozilla Firefox 1.5 et antérieures ;
- Mozilla Thunderbird 1.5 et antérieures ;
- Mozilla Suite 1.7.12 et antérieures.

## 3 Description

Plusieurs vulnérabilités présentes dans les produits Mozilla peuvent être utilisées par un utilisateur mal intentionné pour exécuter du code arbitraire à distance, contourner la politique de sécurité ou encore porter atteinte à la confidentialité de données sur le système vulnérable.

## 4 Solution

En ce qui concerne Mozilla Firefox, il existe une mise à jour, avec la version 1.5.0.1.

En ce qui concerne Mozilla Suite, il est possible de télécharger SeaMonkey 1.0. En effet, la fondation Mozilla a annoncé en mars 2005 la fin du développement de la suite Mozilla. Un groupe indépendant a décidé de continuer le développement de ce logiciel, sous le nom de SeaMonkey.

En ce qui concerne Mozilla Thunderbird, il n'y a pas de mise à jour, mais la recommandation de désactiver le javascript sur Thunderbird.

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

## 5 Documentation

- Site internet de Mozilla :  
<http://www.mozilla.org>
- Bulletin de sécurité Mozilla mfsa2006-01 :  
<http://www.mozilla.org/security/announce/mfsa2006-01.html>
- Bulletin de sécurité Mozilla mfsa2006-02 :  
<http://www.mozilla.org/security/announce/mfsa2006-02.html>
- Bulletin de sécurité Mozilla mfsa2006-03 :  
<http://www.mozilla.org/security/announce/mfsa2006-03.html>
- Bulletin de sécurité Mozilla mfsa2006-04 :  
<http://www.mozilla.org/security/announce/mfsa2006-04.html>
- Bulletin de sécurité Mozilla mfsa2006-05 :  
<http://www.mozilla.org/security/announce/mfsa2006-05.html>
- Bulletin de sécurité Mozilla mfsa2006-06 :  
<http://www.mozilla.org/security/announce/mfsa2006-06.html>
- Bulletin de sécurité Mozilla mfsa2006-07 :  
<http://www.mozilla.org/security/announce/mfsa2006-07.html>
- Bulletin de sécurité Mozilla mfsa2006-08 :  
<http://www.mozilla.org/security/announce/mfsa2006-08.html>
- Référence CVE CAN-2005-4134 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-4134>
- Référence CVE CAN-2006-0292 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2006-0292>
- Référence CVE CAN-2006-0293 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2006-0293>
- Référence CVE CAN-2006-0294 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2006-0294>
- Référence CVE CAN-2006-0295 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2006-0295>
- Référence CVE CAN-2006-0296 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2006-0296>
- Référence CVE CAN-2006-0297 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2006-0297>
- Référence CVE CAN-2006-0298 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2006-0298>
- Référence CVE CAN-2006-0299 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2006-0299>

## Gestion détaillée du document

**03 février 2006** version initiale.

**07 février 2006** rectification de l'erreur de numéro de version corrigeant le problème pour Mozilla Firefox.