



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 13 novembre 2006  
N° CERTA-2006-AVI-482-001

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités des 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-482>

---

### Gestion du document

Référence	CERTA-2006-AVI-482-001
Titre	Vulnérabilités des produits Mozilla
Date de la première version	09 novembre 2006
Date de la dernière version	13 novembre 2006
Source(s)	Avis de sécurité Mozilla MFSA 2006-65 Avis de sécurité Mozilla MFSA 2006-66 Avis de sécurité Mozilla MFSA 2006-67
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 ;
- déni de service à distance ;
- fausses signatures électroniques.

## 2 Systèmes affectés

- Firefox (versions antérieures à 1.5.0.8) ;
- Thunderbird (versions antérieures à 1.5.0.8) ;
- SeaMonkey (versions antérieures à 1.0.6).

## 3 Résumé

La dernière livraison des logiciels Mozilla corrige plusieurs failles de sécurité qui peuvent conduire à l'exécution de code arbitraire ou à de fausses signatures électroniques.

## 4 Description

Plusieurs vulnérabilités ont fait l'objet de correctifs dans les produits Mozilla :

- il a été démontré qu'il était possible de modifier des objets scripts en cours d'exécution. Cette possibilité conduit potentiellement à l'exécution de code JavaScript arbitraire. Cette fonctionnalité touche le moteur du navigateur qui est aussi utilisé dans le lecteur de mail qui devient ainsi vulnérable si la fonctionnalité JavaScript est activée.
- Une vulnérabilité de SeaMonkey permet à un utilisateur distinct d'exécuter à distance du code arbitraire avec les privilèges de l'utilisateur qui utilise ce logiciel.
- Les signatures électronique avec l'algorithme RSA sont falsifiables si l'exposant<sup>1</sup> est trop petit. Cette vulnérabilité est corrigée dans les versions de la bibliothèque de fonctions Network Security Services (NSS) 3.11.3 utilisées dans Firefox 2.0.

## 5 Contournement provisoire

La recommandation générale du CERTA, qui consiste à désactiver par défaut le JavaScript et à ne l'activer qu'au cas par cas, si nécessaire, selon la confiance que l'on accorde aux sites visités, est plus que jamais d'actualité. Cette recommandation générale préconise de ne jamais activer le JavaScript dans un logiciel de courrier électronique.

Si ce n'est pas déjà fait, il est recommandé de désactiver le JavaScript en attendant l'application du correctif de sécurité.

## 6 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation). Le correctif consiste à passer aux versions suivantes des applications vulnérables :

- Firefox 1.5.0.8 ;
- Thunderbird 1.5.0.8 ;
- SeaMonkey 1.0.6.

## 7 Documentation

- Avis de sécurité mozilla MFSA 2006-65 :  
<http://www.mozilla.org/security/announce/2006/mfsa2006-65.html>
- Avis de sécurité mozilla MFSA 2006-66 :  
<http://www.mozilla.org/security/announce/2006/mfsa2006-66.html>
- Avis de sécurité mozilla MFSA 2006-67 :  
<http://www.mozilla.org/security/announce/2006/mfsa2006-67.html>
- Référence CVE CVE-2006-5462 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-5462>
- Référence CVE CVE-2006-5464 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-5464>
- Référence CVE CVE-2006-5747 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-5747>
- Référence CVE CVE-2006-5748 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-5748>
- Avis de sécurité Mandriva MDKSA-2006:205 du 09 novembre 2006 :  
<http://www.mandriva.com/security/advisories?name=MDKSA-2006:205>
- Avis de sécurité Slackware SSA:2006-313-01 du 09 novembre 2006 :  
<http://slackware.com/security/viewer.php?l=slackware-security&y=2006&m=slackware-security.387734>

---

1. La signature électronique RSA repose sur une formule mathématique qui utilise plusieurs nombres. Un de ces nombres s'appelle l'« exposant ».

## **Gestion détaillée du document**

**09 novembre 2006** version initiale.

**13 novembre 2006** ajout des références aux bulletins de sécurité Mandriva et Slackware.