

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités dans différents produits Mozilla et dérivés

---

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-2011-AVI-457>

---

### Gestion du document

Référence	CERTA-2011-AVI-457-001
Titre	Vulnérabilités dans différents produits Mozilla et dérivés
Date de la première version	17 août 2011
Date de la dernière version	23 août 2011
Source	Bulletins de sécurité Mozilla Foundation mfsa2011-29 à mfsa2011-33 du 16 août 2011
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 ;
- contournement de la politique de sécurité ;
- élévation de privilèges.

## 2 Systèmes affectés

- Firefox versions antérieures à 6 ;
- Firefox versions antérieures à 3.6.20 ;
- Thunderbird versions antérieures à 6 ;
- Thunderbird versions antérieures à 3.1.12 ;
- SeaMonkey versions antérieures à 2.3.

Ces vulnérabilités concernent également, sur les distributions Debian :

- iceape, versions antérieures à la version 2.0.11-7 (stable) ou 2.0.14-5 (unstable) ;
- icedove, versions antérieures à la version 3.0.11-1+squeeze4 (stable) ou 3.1.12-1 (unstable) ;
- iceweasel, versions antérieures à la version 3.5.16-9 (stable) ou 6.0-1 (unstable).

### 3 Résumé

De nombreuses vulnérabilités autorisant un utilisateur malintentionné distant à effectuer un déni de service, à exécuter du code arbitraire, à élever ses privilèges ou à contourner la politique de sécurité ont été corrigées dans Firefox, Thunderbird et SeaMonkey.

### 4 Description

De nombreuses vulnérabilités affectant les versions de *Firefox* antérieures à 3.6.20 et à 6 ainsi que les versions de *Thunderbird* antérieures à 6 et à 3.1.12 et les versions de *SeaMonkey* antérieures à 2.3 ont été corrigées.

La vulnérabilité CVE-2011-0084 pourrait permettre d'exécuter du code arbitraire à distance.

La vulnérabilité CVE-2011-2378 fait état d'une erreur dans la gestion des objets DOM pouvant conduire au déréférencement d'un pointeur invalide.

La vulnérabilité CVE-2011-2980 pourrait être exploitée pour charger une bibliothèque dynamique dans un processus hébergeant *Firefox* ou *Thunderbird*.

La faille CVE-2011-2981 autorise une personne malintentionnée à élever ses privilèges.

La vulnérabilité CVE-2011-2982 permet à un utilisateur malintentionné d'exécuter du code à distance.

La faille décrite par le CVE CVE-2011-2983, concerne une violation de la politique de sécurité inter-domaine.

Le CVE CVE-2011-2984 concerne une élévation de privilèges.

Le CVE CVE-2011-2986 concerne une violation de la politique de sécurité inter-domaine pouvant conduire à la fuite d'informations sensibles.

Le CVE-2011-2987 concerne une vulnérabilité autorisant une personne malintentionnée à déclencher un dépassement de tampon dans le tas, menant potentiellement à une exécution de code arbitraire.

La faille décrite dans le CVE CVE-2011-2988 permet d'effectuer un déni de service à distance.

La vulnérabilité CVE-2011-2990 peut conduire à la divulgation d'informations sensibles.

Les vulnérabilités décrites dans les CVE CVE-2011-2989, CVE-2011-2991, CVE-2011-2992 et CVE-2011-2985 permettent à une personne malintentionnée d'exécuter du code arbitraire à distance.

La vulnérabilité CVE-2011-2993 permet d'appeler des fonctionnalités contenues dans une archive `Jar` signée depuis un script non signé. Le script non signé hérite ainsi de l'identité et des privilèges accordés à cette archive par l'utilisateur.

### 5 Solution

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

### 6 Documentation

- Bulletin de sécurité de la fondation Mozilla 2011/mfsa2011-29 du 16 août 2011 :  
<http://www.mozilla.org/security/announce/2011/mfsa2011-29.html>
- Bulletin de sécurité de la fondation Mozilla 2011/mfsa2011-30 du 16 août 2011 :  
<http://www.mozilla.org/security/announce/2011/mfsa2011-30.html>
- Bulletin de sécurité de la fondation Mozilla 2011/mfsa2011-31 du 16 août 2011 :  
<http://www.mozilla.org/security/announce/2011/mfsa2011-31.html>
- Bulletin de sécurité de la fondation Mozilla 2011/mfsa2011-32 du 16 août 2011 :  
<http://www.mozilla.org/security/announce/2011/mfsa2011-32.html>
- Bulletin de sécurité de la fondation Mozilla 2011/mfsa2011-33 du 16 août 2011 :  
<http://www.mozilla.org/security/announce/2011/mfsa2011-33.html>
- Bulletins de sécurité Debian DSA-2295-1 à DSA-2297-1 à du 21 août 2011 :  
<http://www.debian.org/security/2011/dsa-2295>  
<http://www.debian.org/security/2011/dsa-2296>  
<http://www.debian.org/security/2011/dsa-2297>
- Référence CVE CVE-2011-0084 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0084>
- Référence CVE CVE-2011-2378 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2378>

- Référence CVE CVE-2011-2980 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2980>
- Référence CVE CVE-2011-2981 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2981>
- Référence CVE CVE-2011-2982 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2982>
- Référence CVE CVE-2011-2983 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2983>
- Référence CVE CVE-2011-2984 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2984>
- Référence CVE CVE-2011-2985 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2985>
- Référence CVE CVE-2011-2986 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2986>
- Référence CVE CVE-2011-2987 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2987>
- Référence CVE CVE-2011-2988 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2988>
- Référence CVE CVE-2011-2989 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2989>
- Référence CVE CVE-2011-2990 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2990>
- Référence CVE CVE-2011-2991 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2991>
- Référence CVE CVE-2011-2992 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2992>
- Référence CVE CVE-2011-2993 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2993>

## **Gestion détaillée du document**

**17 août 2011** version initiale.

**23 août 2011** ajout des dérivés Debian (iceape, icedove, iceweasel).