Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 09 novembre 2011
N° CERTA-2011-AVI-626

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans les produits Mozilla

Gestion du document

Référence	CERTA-2011-AVI-626
Titre	Multiples vulnérabilités dans les produits Mozilla
Date de la première version	09 novembre 2011
Date de la dernière version	–
Source(s)	Bulletins de sécurité de la fondation Mozilla du 08 novembre 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 ;
- élévation de privilèges ;
- injection de code indirecte à distance.

2 Systèmes affectés

- Firefox versions antérieures à 8.0 ;
- Firefox versions antérieures à 3.6.24 ;
- Thunderbird versions antérieures à 8.0 ;
- Thunderbird versions antérieures à 3.1.16.

3 Résumé

De multiples vulnérabilités ont été corrigées dans les produits de la fondation Mozilla, dont quatre sont considérées comme critiques.

4 Description

De multiples vulnérabilités ont été corrigées dans les produits de la fondation Mozilla:

- mfsa2011-46 : vulnérabilité dans la fonction JSSubScript utilisée par certains modules pouvant être exploitée par du contenu Web malveillant pour élever ses privilèges (cette vulnérabilité a déjà été corrigée dans les branches principales des produits, mais est maintenant également corrigée dans Firefox 3.6.24 et Thunderbird 3.1.16) ;
- mfsa2011-47 : vulnérabilité dans le traitement de données codées en Shift-JIS, pouvant être exploitée pour injecter du code indirectement à distance (XSS) ;
- mfsa2011-48 : plusieurs vulnérabilités dans le moteur de navigation, dont certaines pourraient conduire à une corruption de la mémoire et permettre d'exécuter du code arbitraire à distance dans des circonstances particulières ;
- mfsa2011-49 : arrêt inopiné de Firebug dans le traitement d'un fichier Javascript spécialement conçu ;
- mfsa2011-50 : Problème de confidentialité des données dans l'utilisation de l'accélération graphique Windows D2D ;
- mfsa2011-51 : problème dans les pilotes graphiques sur MacOS X qui peut être exploité par un site Web spécialement conçu pour lire des données antérieures du navigateur ;
- mfsa2011-52 : Vulnérabilité dans NoWaiverWrappers pouvant être exploitée pour une élévation des privilèges.

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/mfsa2011-46 du 08 novembre 2011 : http://www.mozilla.org/security/announce/2011/mfsa2011-46.html
- Bulletin de sécurité de la fondation Mozilla 2011/mfsa2011-47 du 08 novembre 2011 : http://www.mozilla.org/security/announce/2011/mfsa2011-47.html
- Bulletin de sécurité de la fondation Mozilla 2011/mfsa2011-48 du 08 novembre 2011 : http://www.mozilla.org/security/announce/2011/mfsa2011-48.html
- Bulletin de sécurité de la fondation Mozilla 2011/mfsa2011-49 du 08 novembre 2011 : http://www.mozilla.org/security/announce/2011/mfsa2011-49.html
- Bulletin de sécurité de la fondation Mozilla 2011/mfsa2011-50 du 08 novembre 2011 : http://www.mozilla.org/security/announce/2011/mfsa2011-50.html
- Bulletin de sécurité de la fondation Mozilla 2011/mfsa2011-51 du 08 novembre 2011 : http://www.mozilla.org/security/announce/2011/mfsa2011-51.html
- Bulletin de sécurité de la fondation Mozilla 2011/mfsa2011-52 du 08 novembre 2011 : http://www.mozilla.org/security/announce/2011/mfsa2011-52.html
- Référence CVE CVE-2011-3647 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3647
- Référence CVE CVE-2011-3648 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3648
- Référence CVE CVE-2011-3649 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3649
- Référence CVE CVE-2011-3650 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3650
- Référence CVE CVE-2011-3651 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3651
- Référence CVE CVE-2011-3653 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3653
- Référence CVE CVE-2011-3655 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3655

Gestion détaillée du document

09 novembre 2011 version initiale.