



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 10 octobre 2005
N° CERTA-2005-AVI-358-004

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités de Mozilla Firefox et Mozilla Suite

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-2005-AVI-358>

Gestion du document

Référence	CERTA-2005-AVI-358-004
Titre	Vulnérabilités de Mozilla Firefox et Mozilla Suite
Date de la première version	21 septembre 2005
Date de la dernière version	10 octobre 2005
Source(s)	Bulletins de sécurité de 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.

2 Systèmes affectés

- Mozilla Firefox version 1.0.6 et antérieures ;
- Mozilla Suite versions 1.7.11 et versions antérieures.

3 Résumé

Des vulnérabilités dans Mozilla Firefox et dans Mozilla Suite permettent à un utilisateur distant mal intentionné d'exécuter du code arbitraire.

4 Description

Un manque de contrôle dans l'analyse des paramètres passés à Firefox en ligne de commande permet à un utilisateur distant mal intentionné d'exécuter du code arbitraire par le biais d'un lien réticulaire malicieusement construit présent dans une application externe comme un client de messagerie. Remarque : Cette vulnérabilité n'est

exploitable que sur des systèmes de type Unix et GNU/Linux. Plusieurs autres vulnérabilités ont été découvertes dans Mozilla Firefox et Mozilla Suite permettant d'exécuter du code arbitraire à distance.

5 Solution

Mettre à jour Mozilla Firefox en version 1.0.7 et Mozilla Suite en version 1.7.12. Dans tous les cas, se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Site Internet de Mozilla Firefox :
<http://www.mozilla.org/products/firefox/>
- Site Internet de Mozilla Suite :
<http://www.mozilla.org/products/mozilla1.x/>
- Liste des correctifs appliqués dans Mozilla Firefox 1.0.7 :
<http://www.mozilla.org/products/firefox/releases/1.0.7.html>
- Liste des correctifs appliqués dans Mozilla Suite 1.7.12 :
<http://www.mozilla.org/releases/mozilla1.7.12/>
- Bulletin de sécurité Mozilla MFSA 2005-58 du 22 septembre 2005 :
<http://www.mozilla.org/security/announce/mfsa2005-58.html>
- Bulletin de sécurité Mozilla MFSA 2005-59 du 22 septembre 2005 :
<http://www.mozilla.org/security/announce/mfsa2005-59.html>
- Bulletin de sécurité FreeBSD pour mozilla et firefox du 22 septembre 2005 :
<http://www.vuxml.org/freebsd/>
- Bulletin de sécurité RedHat RHSA-2005:785 du 22 septembre 2005 :
<http://rhn.redhat.com/errata/RHSA-2005-785.html>
- Bulletin de sécurité RedHat RHSA-2005:789 du 22 septembre 2005 :
<http://rhn.redhat.com/errata/RHSA-2005-789.html>
- Bulletin de sécurité Mandriva MDKSA-2005:169 du 26 septembre 2005 :
<http://www.mandriva.com/security/advisories?name=MDKSA-2005:169>
- Bulletin de sécurité Mandriva MDKSA-2005:170 du 26 septembre 2005 :
<http://www.mandriva.com/security/advisories?name=MDKSA-2005:170>
- Bulletin de sécurité Debian DSA-838 du 02 octobre 2005 :
<http://www.debian.org/security/2005/dsa-838>
- Référence CVE CAN-2005-2701 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2701>
- Référence CVE CAN-2005-2702 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2702>
- Référence CVE CAN-2005-2703 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2703>
- Référence CVE CAN-2005-2704 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2704>
- Référence CVE CAN-2005-2705 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2705>
- Référence CVE CAN-2005-2706 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2706>
- Référence CVE CAN-2005-2707 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2707>
- Référence CVE CAN-2005-2968 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2968>

Gestion détaillée du document

21 septembre 2005 version initiale.

22 septembre 2005 ajout de la référence au bulletin de sécurité FreeBSD.

23 septembre 2005 ajout des références aux bulletins de sécurité Mozilla, ajout du produit Mozilla Suite, ajout des bulletins de sécurité RedHat et des références CVE.

27 septembre 2005 ajout des références aux bulletins de sécurité Mandriva MDKSA-2005:169 et MDKSA-2005:170.

10 octobre 2005 ajout de la référence au bulletin de sécurité Debian DSA-838.