



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 14 mai 2004
N° CERTA-2004-AVI-080-002

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans 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-2004-AVI-080>

Gestion du document

Référence	CERTA-2004-AVI-080-002
Titre	Multiples vulnérabilités dans Mozilla
Date de la première version	11 mars 2004
Date de la dernière version	14 mai 2004
Source(s)	Avis MDKSA-2004:021 de Mandrake
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

- Accès non sollicité ;
- déni de service ;
- exécution de code arbitraire à distance.

2 Systèmes affectés

Mozilla 1.4.

3 Résumé

Plusieurs vulnérabilités ont été découvertes dans le navigateur Mozilla.

4 Description

Plusieurs vulnérabilités affectent Mozilla de la façon suivante :

- un site malicieux peut contourner les mécanismes d'authentification d'un serveur mandataire ;

- une vulnérabilité présente dans les scripts `Script.prototype.freeze` et `Script.prototype.thaw` permet à un utilisateur mal intentionné d'exécuter du code arbitraire à distance ;
- NSS (Network Security Suite) est un ensemble de bibliothèques offrant des fonctions de chiffrement au navigateur. Une vulnérabilité présente dans la mise en œuvre de S/MIME permet à un individu mal intentionné d'effectuer un déni de service ou bien d'exécuter du code arbitraire à distance à l'aide d'un mél malicieusement constitué ;
- une vulnérabilité dans le mécanisme de gestion des cookies permet à un utilisateur mal intentionné de contourner les restrictions spécifiées sur les chemins.

5 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs :

- Avis MDKSA-2004:021 de Mandrake :
<http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2004:021>
- Avis RHSA-2004:112 de Red Hat :
<http://rhn.redhat.com/errata/RHSA-2004-112.html>
- Bulletin de sécurité HPSBTU01021 pour HP Tru64 UNIX :
<http://www.itrc.hp.com>
- Bulletin de sécurité HPSBUX01036 pour HP-UX :
<http://www.itrc.hp.com>

6 Documentation

- Référence CVE CAN-2003-0594 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0594>
- référence CVE CAN-2003-0564 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0564>
- Avis CERTA-2004-AVI-081 du CERTA :
<http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-081/>

Gestion détaillée du document

11 mars 2004 version initiale.

19 mars 2004 ajout référence au bulletin de sécurité de Red Hat.

14 mai 2004 ajout références aux bulletins de sécurité relatifs à HP Tru64 UNIX et HP-UX.