

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité du navigateur 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-2005-AVI-007>

Gestion du document

Référence	CERTA-2005-AVI-007-002
Titre	Vulnérabilité du navigateur Mozilla
Date de la première version	05 janvier 2005
Date de la dernière version	14 janvier 2005
Source(s)	Bulletin de sécurité iSec du 29 décembre 2004
Pièce(s) jointe(s)	

TAB. 1 – Gestion du document

Une gestion de version détaillée se trouve à la fin de ce document.

1 Risque

Exécution de code arbitraire.

2 Systèmes affectés

Mozilla 1.7.3 et versions antérieures.

3 Résumé

Une vulnérabilité présente dans le navigateur Internet Mozilla permet à une personne mal intentionnée d'exécuter du code arbitraire à distance.

4 Description

Le navigateur Mozilla présente une vulnérabilité dans la gestion du protocole NNTP. Un utilisateur mal intentionné peut exécuter du code arbitraire à distance sur le système vulnérable, au moyen d'un site web ou d'une adresse réticulaire (URL) malicieusement constitué.

5 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. Documentation).

6 Documentation

- Site Internet de l'éditeur Mozilla :
<http://www.mozilla.org/>
- Bulletin de sécurité iSec "Heap overflow in Mozilla Browser <= 1.7.3 NNTP code" du 29 décembre 2004 :
<http://isec.pl/vulnerabilities/isec-0020-mozilla.txt>
- Mise à jour Mozilla 1.7.5 :
<http://www.mozilla.org/releases/#1.7.5>
- Bulletin de sécurité Gentoo GLSA 200501-03 du 05 janvier 2005 :
<http://www.gentoo.org/security/en/glsa/glsa-200501-03.xml>
- Bulletin de sécurité RedHat RHSA-2005:038 du 13 janvier 2005 :
<http://rhn.redhat.com/errata/RHSA-2005-038.html>
- Référence CVE CAN-2004-1316 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1316>

Gestion détaillée du document

05 janvier 2005 version initiale.

07 janvier 2005 ajout de la référence au bulletin de sécurité de Gentoo.

14 janvier 2005 ajout de la référence au bulletin de sécurité de RedHat et à la référence CVE CAN-2004-1316.