



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 05 octobre 2005
N° CERTA-2005-AVI-346-002

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité des clients web Mozilla, Firefox, Netscape et du client mail Thunderbird

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-346>

Gestion du document

Référence	CERTA-2005-AVI-346-002
Titre	Vulnérabilité des clients web Mozilla, Firefox, Thunderbird et Netscape
Date de la première version	15 septembre 2005
Date de la dernière version	05 octobre 2005
Source(s)	Avis Security-Protocols du 08 septembre 2005
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

- Dénis de service ;
- exécution potentielle de code arbitraire à distance.

2 Systèmes affectés

Tout système - quel que soit le système d'exploitation - utilisant un butineur Mozilla, Mozilla-Firefox ou Netscape.

La vulnérabilité existe mais ne peut être exploitée par défaut sur le client de messagerie Mozilla Thunderbird.

3 Résumé

Il est possible de créer une page web contenant un lien volontairement mal formé qui va bloquer le butineur. L'exécution de code avec les privilèges de l'utilisateur courant n'est pas exclue.

4 Description

Une erreur dans la prise en compte des noms de domaines internationaux (« IDN », extension des noms de domaine à des caractères non ASCII) peut provoquer un débordement de tampon en mémoire.

5 Contournement provisoire

Désactiver le support d'IDN dans le butineur (voir le vendeur Mozilla dans la section Documentation) en exécutant le correctif proposé ou en éditant la configuration à l'aide de la commande `about:config` dans la barre de navigation et en positionnant la valeur `network.enableIDN` à `false`.

6 Solution

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

7 Documentation

- Site internet des butineurs Mozilla, Firefox et Thunderbird :
<http://www.mozilla.org>
- Contournement provisoire en désactivant le support d'IDN :
 - Procédure (en anglais) :
<http://www.mozilla.org/security/idn.html>
 - Correctif provisoire à exécuter :
<ftp://ftp.mozilla.org/pub/mozilla.org/firefox/releases/1.0.6/patches/307259.xpi>
- Bulletins de sécurité Red Hat Linux :
 - RHSA-2005-768 du 09 septembre 2005 pour Firefox :
<http://rhn.redhat.com/errata/RHSA-2005-768.html>
 - RHSA-2005-769 du 09 septembre 2005 pour Mozilla :
<http://rhn.redhat.com/errata/RHSA-2005-769.html>
- Bulletins de sécurité Linux Fedora :
 - Mise à jour de sécurité pour Fedora Core 3 du 10 septembre 2005 :
<http://www.securityfocus.com/advisories/9236>
 - Mise à jour de sécurité pour Fedora Core 4 du 10 septembre 2005 :
<http://www.securityfocus.com/advisories/9235>
- Bulletin de sécurité Debian DSA-837 :
<http://www.debian.org/security/2005/dsa-837>
- Avis Security-Protocols du 08 septembre 2005 :
<http://security-protocols.com/advisory/sp-x17-advisory.txt>
- Note de vulnérabilité VU#573857 de l'US-CERT :
<http://www.kb.cert.org/vuls/id/573857>
- Bulletins de sécurité HP-UX :
 - SSRT051040 :
<http://www1.itrc.hp.com/service/cki/docDisplay.do?docId=HPSBUX01230>
 - SSRT051041 :
<http://www1.itrc.hp.com/service/cki/docDisplay.do?docId=HPSBUX01231>
- Référence CVE CAN-2005-2871 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2871>

Gestion détaillée du document

15 septembre 2005 version initiale.

03 octobre 2005 ajout de la référence au bulletin de sécurité Debian.

04 octobre 2005 ajout de Mozilla Thunderbird dans la section “Systèmes affectés”.

05 octobre 2005 ajout de la référence au bulletin HP-UX.