Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 28 novembre 2005
N° CERTA-2005-AVI-438-002

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité du logiciel Macromedia Flash Player

Gestion du document

Référence	CERTA-2005-AVI-438-002
Titre	Vulnérabilité du logiciel Macromedia Flash Player
Date de la première version	07 novembre 2005
Date de la dernière version	28 novembre 2005
Source(s)	Bulletin de sécurité de Macromedia
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 commandes arbitraires via un site web malicieux ;
– exécution de commandes arbitraires via un fichier SWF malicieux.

2 Systèmes affectés

Macromedia Flash Player version 7.0.19.0 et versions inférieures.

3 Description

Une vulnérabilité a été découverte dans la gestion des variables des fichiers SWF du logiciel Macromedia Flash Player.

Cette vulnérabilité peut être exploitée afin d'exécuter du code arbitraire via un site web ou un fichier SWF malicieusement construit.

4 Solution

Deux solutions peuvent être envisagées :
– Utiliser Flash player 8 (version 8.0.22.0) ;

– mettre à jour Flash Player 7 en version 7.0.61.0 ou 7.0.60.0.

5 Documentation

– Site de l'éditeur :
http://www.macromedia.com
– Bulletin de sécurité Eeye du 04 novembre 2005 :
http://www.eeye.com/html/research/advisories/AD20051104.html
– Bulletin de sécurité de l'éditeur :
http://www.macromedia.com/devnet/security/security_zone/mpsb05-07.html
– Mises à jour de sécurité FreeBSD pour linux-flashplugin6 et linux-flashplugin7 du 13 novembre 2005 :
http://www.vuxml.org/freebsd/pkg-linux-flashplugin6.html
http://www.vuxml.org/freebsd/pkg-linux-flashplugin7.html
– Bulletin de sécurité Gentoo GLSA 200511-21 du 25 novembre 2005 :
http://www.gentoo.org/security/en/glsa/glsa-200511-21.xml
– Référence CVE CAN-2005-2628 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2628

Gestion détaillée du document

07 novembre 2005 version initiale.

21 novembre 2005 ajout de la référence au bulletin de sécurité Eeye et des mises à jour de sécurité FreeBSD.

28 novembre 2005 ajout de la référence au bulletin de sécurité Gentoo GLSA 200511-21 et de la réference CVE CAN-2005-2628.