



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 18 octobre 2007
N° CERTA-2007-AVI-444

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans IrfanView

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-2007-AVI-444>

Gestion du document

Référence	CERTA-2007-AVI-444
Titre	Vulnérabilité dans IrfanView
Date de la première version	18 octobre 2007
Date de la dernière version	–
Source(s)	Avis de changement de version 4.10 IrfanView du 15 octobre 2007
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 ;
- contournement de la politique de sécurité.

2 Systèmes affectés

- IrfanView version 3.99 ;
- IrfanView version 4.00.

3 Résumé

Une vulnérabilité a été identifiée dans le logiciel de manipulation d'images IrfanView. Elle permettrait à une personne malveillante d'exécuter, par le biais d'un fichier spécialement construit, du code arbitraire sur le système ayant une version vulnérable.

4 Description

Une vulnérabilité a été identifiée dans le logiciel de manipulation d'images IrfanView. Il ne manipulerait pas correctement des fichiers au format .PAL définissant des palettes de couleurs.

Cette vulnérabilité pourrait être exploitée par une personne malveillante avec un fichier .pal spécialement construit. Son importation dans une version d'IrfanView vulnérable permettrait alors l'exécution de code sur le système.

5 Solution

Se référer au bulletin de mise à jour pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Avis de changement de version 4.10 IrfanView du 15 octobre 2007 :
<http://www.irfanview.com>
- Alerte de Secunia numéro 2007-71 du 16 octobre 2007 :
http://secunia.com/secunia_research/2007-71/advisory/
- Référence CVE CVE-2007-4343 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-4343>

Gestion détaillée du document

18 octobre 2007 version initiale.