



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 16 avril 2010
N° CERTA-2010-ALE-005-001

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Vulnérabilité dans Java Deployment Toolkit

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-2010-ALE-005>

Gestion du document

Référence	CERTA-2010-ALE-005-001
Titre	Vulnérabilité dans Java Deployment Toolkit
Date de la première version	09 avril 2010
Date de la dernière version	16 avril 2010
Source(s)	–
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.

2 Systèmes affectés

Java Deployment Toolkit sous Windows.

3 Résumé

Une vulnérabilité dans Java Deployment Toolkit permet à un utilisateur malveillant d'exécuter du code arbitraire à distance.

4 Description

Java Deployment Toolkit comprend un ActiveX pour internet Explorer et un greffon pour Firefox destinés à faciliter le déploiement d'applications Java. Il offre une fonction qui permet de donner un argument au gestionnaire des fichiers JNLP (*Java Networking Launching Protocol*). Dans une configuration standard, ce gestionnaire est le

programme Java Web Start. La faiblesse du filtrage offert par la fonction de lancement permet à un utilisateur malveillant d'exécuter du code arbitraire à distance.

Le savoir-faire nécessaire à l'exploitation de cette vulnérabilité est disponible sur Internet. Des attaques l'utiliseraient d'ores et déjà.

5 Contournement provisoire

Pour réduire la possibilité d'exploiter cette vulnérabilité, il est recommandé, sous réserve des contraintes opérationnelles :

- de désinstaller le Java Deployment Toolkit ;
- de désinstaller Java Web Start s'il n'est pas utilisé ;
- de positionner le *killbit* sur l'objet (CLSID) `CAFEEEFAC-DEC7-0000-0000-ABCDEFEDCBA` ;
- de positionner des droits d'accès réduits sur la bibliothèque dynamiques `npdeploytk.dll`.

L'impact est minimisé lorsque l'utilisateur ne dispose que de droits restreints.

6 Solution

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

7 Documentation

- Prévention de l'exécution d'un ActiveX depuis Internet Explorer :
<http://support.microsoft.com/kb/240797>
- Bulletin de sécurité du CERTA CERTA-010-AVI-185 du 16 avril 2010 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2010-AVI-185/index.html>
- Bulletin de sécurité Oracle CVE-2010-0886 du 15 avril 2010 :
<http://www.oracle.com/technology/deploy/security/alerts/alert-cve-2010-0886.html>
- Notes de mise à jour Sun JAVA 1.6.0_20 du 15 avril 2010 :
<http://java.sun.com/javase/6/webnotes/6u20.html>
- Référence CVE CVE-2010-0886 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0886>
- Référence CVE CVE-2010-0887 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0887>

Gestion détaillée du document

09 avril 2010 version initiale.

16 avril 2010 publication du correctif.