

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités de la Machine Virtuelle de Microsoft

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-2002-AVI-265>

Gestion du document

Référence	CERTA-2002-AVI-265
Titre	Multiples vulnérabilités de la Machine Virtuelle de Microsoft
Date de la première version	13 décembre 2002
Date de la dernière version	–
Source(s)	Bulletin de sécurité MS02-069 de Microsoft
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

- Dénier de service ;
- contournement des règles de sécurité ;
- fuite de données ;
- modification de données non autorisée ;
- exécution de code arbitraire à distance.

2 Systèmes affectés

Tous les systèmes Microsoft possédant une version de la Machine Virtuelle (VM) inférieure à 5.0.3805 incluse.
Pour connaître la version de la Machine Virtuelle de vos systèmes, consultez le document additionnel référencé dans le bulletin de sécurité MS02-069 de Microsoft :

http://www.microsoft.com/security/security_bulletins/ms02-069.asp

3 Résumé

De multiples vulnérabilités présentes dans la Machine Virtuelle de Microsoft permettent à un utilisateur mal intentionné d'exécuter du code arbitraire à distance, de contourner les mécanismes de sécurité et d'obtenir des informations sur l'utilisateur, ce qui pourrait faciliter les attaques par force brute.

4 Description

La Machine Virtuelle de Microsoft a pour objet d'exécuter des programmes Java.

De multiples vulnérabilités sont présentes dans la Machine Virtuelle de Microsoft pour les versions 5.0.3805 et antérieures :

- Le standard COM (*Composant Object Model*) permet de gérer la modularité de certaines applications sous Windows.
Seules les appliquestes Java « de confiance » (ou reconnues comme sûres) peuvent accéder aux objets COM
L'une des vulnérabilités de la Machine Virtuelle permet aux appliquestes Java « non reconnues comme sûres » d'accéder aux objets COM.
- Une appliqueste Java ne peut normalement accéder qu'au répertoire dans lequel elle se situe ou aux sous-répertoires de ce dernier. Il est possible de construire (par deux moyens différents) une appliqueste Java qui « tromperait » la Machine Virtuelle sur son emplacement lorsqu'elle est exécutée, et pourrait accéder à des objets situés dans des répertoires distants.
- Il est aussi possible de construire une URL qui, lors de son traitement, permet l'exécution d'une appliqueste Java dans un autre domaine que celui depuis lequel elle est lancée. Ceci peut notamment être utilisé pour exécuter une application Java dans un contexte de sécurité différent de celui pour lequel elle est autorisée.
- Les API (*Application Programming Interface*) JDBC (*Java DataBase Connectivity*) sont des applications permettant d'accéder à des bases de données (ajout, modification, destruction) par le biais de programmes JAVA.
Une vulnérabilité de la Machine Virtuelle permet à une appliqueste Java d'accéder aux applications JDBC.
- Le SSM (*Security Standard Manager*) est un outil permettant d'appliquer des restrictions sur l'accès de certains objets Java.
Une vulnérabilité de la Machine Virtuelle permet d'empêcher temporairement l'exécution de certains de ces objets en modifiant la « banlist » (liste des objets bannis).
- Il est possible d'obtenir le nom de l'utilisateur connecté sur un système grâce à une appliqueste Java « non reconnue comme sûre » qui ne devrait normalement pas permettre d'accéder à une propriété du système nommée `user.dir`.
- Une création non terminée d'objet Java par une autre appliqueste Java habilement construite permet d'arrêter de façon inopinée le navigateur Internet Explorer.

5 Contournement provisoire

Pour se prémunir contre la majeure partie de ces attaques via le navigateur Internet Explorer, désactiver les appliquestes Java dans les paramètres de sécurité de tous les contextes de sécurité d'Internet Explorer.

6 Solution

Consulter le bulletin de sécurité MS02-069 (se référer au paragraphe documentation) afin de connaître la disponibilité des correctifs.

7 Documentation

Bulletin de sécurité MS02-069 de Microsoft et son document additionnel :

<http://www.microsoft.com/technet/security/bulletin/MS02-069.asp>

http://www.microsoft.com/security/security_bulletins/ms02-069.asp

Gestion détaillée du document

13 décembre 2002 version initiale.