

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Débordement de mémoire dans l'application ASP . NET 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-120>

---

### Gestion du document

Référence	CERTA-2002-AVI-120
Titre	Débordement de mémoire dans l'application ASP . NET de Microsoft
Date de la première version	10 juin 2002
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS02-026
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 ;
- déni de service.

## 2 Systèmes affectés

Tous les serveurs web équipés de l'outil ASP . NET.

## 3 Résumé

Un utilisateur mal intentionné peut effectuer un débordement de mémoire à distance et exécuter du code arbitraire sur un serveur utilisant l'outil ASP . NET.

## 4 Description

ASP . NET est un outil de développement d'applications web.

Parmi les modes d'ASP.NET, le mode `StateServer` permet de gérer des sessions en stockant des informations sur l'état de chaque session ouverte.

Un débordement de mémoire dans une fonction de gestion de *cookies* d'ASP.NET en mode `StateServer` permet à un utilisateur mal intentionné d'exécuter du code arbitraire à distance dans le contexte de sécurité d'ASP.NET dont le compte ne possède normalement aucun privilège.

Le mode `StateServer` n'est pas activé par défaut lors de l'installation d'ASP.NET.

## 5 Contournement provisoire

- Désactiver les cookies d'ASP.NET en mode `StateServer` ;
- ne pas utiliser le mode `StateServer` si cela est possible.

## 6 Solution

Appliquer le correctif de Microsoft :

<http://www.microsoft.com/Downloads/Release.asp/ReleaseID=39298>

## 7 Documentation

Bulletin de sécurité Microsoft MS02-026 :

<http://www.microsoft.com/technet/security/bulletin/MS02-026.asp>

## Gestion détaillée du document

10 juin 2002 version initiale.