



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 09 février 2005
N° CERTA-2005-AVI-055

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité d'authentification dans ASP.NET

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-2005-AVI-055>

Gestion du document

Référence	CERTA-2005-AVI-055
Titre	Vulnérabilité d'authentification dans ASP.NET
Date de la première version	09 février 2005
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS05-004
Pièce(s) jointe(s)	

TAB. 1 – Gestion du document

Une gestion de version détaillée se trouve à la fin de ce document.

1 Risque

- Contournement de la politique de sécurité ;
- atteinte à la confidentialité des données ;
- élévation de privilège.

2 Systèmes affectés

- .NET Framework 1.0 ;
- .NET Framework 1.1 ;
- ASP.NET.

3 Résumé

Une vulnérabilité présente dans les sites web créés à l'aide des outils de développement ASP.NET et .NET Framework permet à un utilisateur mal intentionné d'obtenir un accès non autorisé à un site web vulnérable.

4 Description

Les outils de développement ASP.NET et .NET Framework permettent de créer des sites web avec un contenu dynamique.

Une vulnérabilité découverte dans le système d'authentification des sites web ASP.NET permet à un utilisateur distant mal intentionné de contourner la sécurité mise en place sur ce site afin de porter atteinte à la confidentialité des données ou toute autre action rendue possible par le contenu de la page accédée.

5 Solution

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

6 Documentation

- Bulletin de sécurité de Microsoft MS05-004 du 08 février 2005 :
<http://www.microsoft.com/technet/security/bulletin/MS05-004.msp>
- Référence CVE CAN-2004-0847 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0847>

Gestion détaillée du document

09 février 2005 version initiale.