Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 30 décembre 2011
N° CERTA-2011-AVI-727

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans l'implémentation ASP.Net du Microsoft .NET Framework

Gestion du document

Référence	CERTA-2011-AVI-727
Titre	Vulnérabilités dans l'implémentation ASP.Net du Microsoft .NET Framework
Date de la première version	30 décembre 2011
Date de la dernière version	–
Source(s)	Avis de sécurité MS11-100
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

- Déni de service à distance ;
- Usurpation d'identité ;
- élévation de privilèges.

2 Systèmes affectés

- Microsoft .NET Framework 1.0 Service Pack 3 ;
- Microsoft .NET Framework 1.1 Service Pack 1 ;
- Microsoft .NET Framework 2.0 Service Pack 2 ;
- Microsoft .NET Framework 3.5 Service Pack 1 ;
- Microsoft .NET Framework 3.5.1 ;
- Microsoft .NET Framework 4.

3 Résumé

Microsoft a publié un bulletin de sécurité adressant 4 vulnérabilités dans le *Microsoft Framework .NET*. Les plus sévères de ces vulnérabilités permettent l'élévation de privilège et le déni de service à distance pour les applications *ASP.Net*.

4 Description

Quatre vulnérabilités ont été corrigées dans ASP.Net.
Leur exploitation réussie conduit à:

- l'élévation de privilège à distance via l'usurpation d'un compte existant d'un site reposant sur l'authentification par formulaire ;
- un déni de service par épuisement des resources processeur du serveur ;
- une redirection de l'utilisateur vers un site arbitraire lors de l'authentification par formulaire sur un site web.

Les détails techniques de l'attaque par déni de service ont été publiées et peuvent conduire rapidement au développement d'outils exploitant cette vulnérabilité. Des informations complémentaires sont fournies sur cette technique d'attaque dans le bulletin d'actualité CERTA-2011-ACT-052 (cf. section Documentation).

5 Contournement provisoire

Le bulletin de l'éditeur suggère plusieurs contournements provisoires. Le CERTA recommande une revue détaillée de ces contournements avant toute mise en production. En effet, il s'agit parfois de désactiver les mécanismes d'authentification mis en place sur la plateforme (pour les vulnérabilités d'usurpation d'identité) ou encore de restreindre la longueur des requêtes acceptées par le serveur. Ces contournements peuvent être contre-productifs en termes de sécurité et de disponibilité. Dans tous les cas, le CERTA recommande l'installation des correctifs proposés par l'éditeur lorsqu'ils sont disponibles.

L'article KB318785 de la base de connaissance *Microsoft* documente les moyens de déterminer les versions du *Microsoft Framework .NET* (cf. section Documentation)

6 Solution

Note: Toutes les versions du *Microsoft Framework .NET* sont affectées. Plusieurs versions du composant peuvent cohabiter sur un même poste et doivent donc individuellement être mises à jour.

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

7 Documentation

- Bulletin de sécurité Microsoft MS11-100 du 29 décembre 2011 :
  http://technet.microsoft.com/fr-fr/security/bulletin/MS11-100
  http://technet.microsoft.com/en-us/security/bulletin/MS11-100
- Bulletin d'actualité du CERTA du 30 décembre 2011 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2011-ACT-052
- Article de la base de connaissance Microsoft KB318785 :
  http://support.microsoft.com/kb/318785

Gestion détaillée du document

30 décembre 2011 version initiale.