



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 décembre 2009
N° CERTA-2009-AVI-536

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans Microsoft ADFS

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-2009-AVI-536>

Gestion du document

Référence	CERTA-2009-AVI-536
Titre	Vulnérabilités dans Microsoft ADFS
Date de la première version	09 décembre 2009
Date de la dernière version	–
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 ;
- contournement de la politique de sécurité.

2 Systèmes affectés

- Windows Server 2003 avec ADFS activé, toutes éditions, (*Windows Server 2003 R2*) ;
- Windows Server 2008, toutes éditions.

3 Résumé

Deux vulnérabilités présentes dans ADFS (*Active Directory Federation Service*) ont été publiées. La plus importante permet à un utilisateur malveillant d'exécuter du code arbitraire à distance.

4 Description

- Deux vulnérabilités présentes dans ADFS (*Active Directory Federation Service*) ont été publiées :
- la première permet à un utilisateur malveillant d'usurper l'identité d'un utilisateur légitime, sous réserve

- d'accéder à un poste client depuis lequel ce dernier s'est connecté et d'avoir activé la fonction d'identification unique (SSO, *Single Sign-On*) sur le serveur vulnérable ;
- la seconde réside dans le traitement des requêtes des utilisateurs authentifiés. Elle permet à un utilisateur malveillant ayant des informations de connexion valides de prendre le contrôle du serveur vulnérable, à distance.

5 Solution

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

6 Documentation

- Bulletin de sécurité Microsoft MS09-070 du 08 décembre 2009 :
<http://www.microsoft.com/france/technet/security/Bulletin/MS09-070.mspix>
<http://www.microsoft.com/technet/security/Bulletin/MS09-070.mspix>
- Référence CVE CVE-2009-2508 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2508>
- Référence CVE CVE-2009-2509 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2509>

Gestion détaillée du document

09 décembre 2009 version initiale.