



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 12 octobre 2011  
N° CERTA-2011-AVI-556

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités dans Microsoft Forefront Unified Access Gateway

---

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-2011-AVI-556>

---

### Gestion du document

Référence	CERTA-2011-AVI-556
Titre	Vulnérabilités dans Microsoft Forefront Unified Access Gateway
Date de la première version	12 octobre 2011
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS11-079 du 11 octobre 2011
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 à distance ;
- injection de code indirecte à distance.

## 2 Systèmes affectés

- Microsoft Forefront Unified Access Gateway 2010 ;
- Microsoft Forefront Unified Access Gateway 2010 Update 1 ;
- Microsoft Forefront Unified Access Gateway 2010 Update 2 ;
- Microsoft Forefront Unified Access Gateway 2010 Service Pack 1.

## 3 Résumé

Plusieurs vulnérabilités dans Microsoft Forefront Unified Access Gateway permettent à une personne distante malintentionnée d'exécuter du code arbitraire, de provoquer un déni de service ou d'effectuer des injections de code indirectes.

## 4 Description

Cinq vulnérabilités ont été découvertes dans Microsoft Forefront Unified Access Gateway :

- trois vulnérabilités permettent d'effectuer des injections de code indirectes (XSS) (CVE-2011-1895, CVE-2011-1896 et CVE-2011-1897) ;
- une vulnérabilité dans une applique Java utilisée par Microsoft Forefront Unified Gateway Access permet à une personne distante malintentionnée d'exécuter du code arbitraire (CVE-2011-1969) ;
- une vulnérabilité dans la gestion des fichiers de session (*cookie*) permet de provoquer un déni de service *IIS* (CVE-2011-2012).

## 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 MS11-079 du 11 octobre 2011 :  
<http://technet.microsoft.com/fr-fr/security/bulletin/MS11-079>  
<http://www.microsoft.com/technet/security/Bulletin/MS11-079.msp>
- Référence CVE CVE-2011-1869 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1869>
- Référence CVE CVE-2011-1895 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1895>
- Référence CVE CVE-2011-1896 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1896>
- Référence CVE CVE-2011-1897 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1897>
- Référence CVE CVE-2011-2012 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2012>

## Gestion détaillée du document

12 octobre 2011 version initiale.