

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-2010-AVI-545>

Gestion du document

Référence	CERTA-2010-AVI-545
Titre	Vulnérabilités dans Microsoft Forefront Unified Access Gateway
Date de la première version	10 novembre 2010
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS10-089 du 09 novembre 2010
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

- Contournement de la politique de sécurité ;
- injection de code indirecte à distance ;
- élévation de privilèges.

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.

3 Résumé

Plusieurs vulnérabilités corrigées dans Microsoft Forefront Unified Access Gateway 2010 permettent à un utilisateur malveillant d'élever ses privilèges ou de contourner la politique de sécurité.

4 Description

Plusieurs vulnérabilités ont été corrigées dans Microsoft Forefront Unified Access Gateway 2010 :

- Une vulnérabilité permet à un utilisateur malintentionné, par le biais d'un lien spécialement conçu, de rediriger le trafic du serveur Web vers un site malveillant (CVE-2010-2732) ;
- plusieurs vulnérabilités permettent à un utilisateur malintentionné, par le biais d'un lien spécialement conçu, d'exécuter certaines commandes sur le serveur (CVE-2010-2733, CVE-2010-2734 et CVE-2010-3936).

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 MS10-089 du 09 novembre 2010 :
<http://www.microsoft.com/france/technet/security/Bulletin/MS10-089.msp>
<http://www.microsoft.com/technet/security/Bulletin/MS10-089.msp>
- Référence CVE CVE-2010-2732 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2732>
- Référence CVE CVE-2010-2733 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2733>
- Référence CVE CVE-2010-2734 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2734>
- Référence CVE CVE-2010-3936 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3936>

Gestion détaillée du document

10 novembre 2010 version initiale.