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 2011
N° CERTA-2010-ALE-021-003

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Vulnérabilité dans Microsoft Internet Explorer

Gestion du document

Référence	CERTA-2010-ALE-021-003
Titre	Vulnérabilité dans Microsoft Internet Explorer
Date de la première version	22 décembre 2010
Date de la dernière version	09 février 2011
Source(s)	Bulletin de Sécurité Microsoft 2488013 du 22 décembre 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

- Exécution de code arbitraire à distance ;
- déni de service à distance.

2 Systèmes affectés

- Microsoft Internet Explorer 6 ;
- Microsoft Internet Explorer 7 ;
- Microsoft Internet Explorer 8.

3 Résumé

L'éditeur a publié un correctif le 08 février 2011.

Une vulnérabilité dans Microsoft Internet Explorer permet à un utilisateur malveillant d'exécuter du code arbitraire à distance par l'intermédiaire d'une page web spécialement conçue.

4 Description

Une vulnérabilité affecte Microsoft Internet Explorer et permet à un utilisateur malveillant d'exécuter du code arbitraire à distance en utilisant des feuilles de style (CSS) spécialement conçues.

Une preuve de faisabilité est déjà disponible sur l'Internet.

5 Contournement provisoire

Dans l'attente d'un correctif de l'éditeur, le CERTA recommande plusieurs actions :

- pour limiter la possibilité d'exploitation de la vulnérabilité :
  - la désactivation de l'interprétation des scripts Javascript ;
  - le déploiement d'EMET (*Enhanced Mitigation Experience Toolkit*) ;
  - l'utilisation d'un navigateur alternatif ;
- pour limiter l'impact de l'exploitation de la vulnérabilité, l'utilisation d'un compte utilisateur avec des droits restreints.

Microsoft a publié le correctif `MicrosoftFixIt50591.msi` afin d'aller éditer temporairement la bibliothèque partagée `MSHTML.DLL`, responsable de cette vulnérabilité. Pour pouvoir appliquer ce correctif il est nécessaire d'appliquer les dernières mises à jour de sécurité, notamment le correctif MS10-090 du 14 décembre 2010.

Il est également nécessaire de bien mesurer les effets de bord possibles de ce correctif avant tout déploiement en production.

6 Solution

L'éditeur a publié le correctif MS11-003 pour corriger cette vulnérabilité.
Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

7 Documentation

- Bulletin de sécurité Microsoft MS11-003 du 08 février 2011 :
  http://www.microsoft.com/france/technet/security/Bulletin/MS11-003.mspx
  http://www.microsoft.com/technet/security/Bulletin/MS11-003.mspx
- Bulletin de sécurité Microsoft 2488013 du 22 décembre 2010 :
  http://www.microsoft.com/technet/security/advisory/2488013.mspx
- Bloc-Notes Microsoft SRD, "New Internet Explorer vulnerability affecting all versions of IE", 22 décembre 2010 :
  http://blogs.technet.com/b/srd/archive/2010/12/22/new-internet-explorer-vulnerability-affecting-all-versions-of-ie.aspx
- Bloc-Notes Microsoft SRD, "New workaround included in security Advisory 2488013", 11 janvier 2011 :
  http://blogs.technet.com/b/srd/archive/2011/01/11/new-workaround-included-in-security-advisory-2488013.aspx
- Document du CERTA CERTA-2011-AVI-058 du 09 février 2011 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2011-AVI-058/
- Référence CVE CVE-2010-3971 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3971

Gestion détaillée du document

22 décembre 2010 version initiale.

23 décembre 2010 ajout de la référence au bulletin Microsoft et de la référence CVE.

12 janvier 2011 ajout du correctif temporaire dans les contournements provisoires.

09 février 2011 ajout du correctif MS11-003.