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 août 2009
N° CERTA-2009-ALE-011-001

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Vulnérabilité dans Microsoft Office Web Components Control

Gestion du document

Référence	CERTA-2009-ALE-011-001
Titre	Vulnérabilité dans Microsoft Office Web Components Control
Date de la première version	13 juillet 2009
Date de la dernière version	12 août 2009
Source(s)	Bulletin de sécurité Microsoft 973472 du 13 juillet 2009
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.

2 Systèmes affectés

- Microsoft Office XP SP3 ;
- Microsoft Office 2003 SP3 ;
- Microsoft Office XP Web Components SP3 ;
- Microsoft Office 2003 Web Components SP3 ;
- Microsoft Office Web Component pour Microsoft Office 2007 SP1 ;
- Microsoft Internet Security and Acceleration Server 2004 Standard & Enerprise Edition SP3 ;
- Microsoft Internet Security and Acceleration Server 2006 ;
- Internet Security and Acceleration Server 2006 Supportability Update ;
- Microsoft Internet Security and Acceleration Server 2006 SP1 ;
- Microsoft Office Small Business Accounting 2006.

3 Résumé

Une vulnérabilité dans *Microsoft Office Web Components Control* permet à un utilisateur malveillant d'exécuter du code arbitraire à distance.

4 Description

Une vulnérabilité de nature non précisée par l'éditeur dans *Microsoft Office Web Components Control* permet à une personne malintentionnée distante d'exécuter du code arbitraire, avec les droits de l'utilisateur, au moyen d'une page web spécialement écrite visualisée dans *Internet Explorer*.

5 Contournement provisoire

Les moyens de contournement suivants sont disponibles :

- `Microsoft` a publié un contournement provisoire afin de désactiver le composant mis en cause. Une application est disponible sur le bulletin de sécurité `Microsoft` (cf. la section Documentation). Afin de désactiver le composant, il faut placer la valeur *Compatibility Flags* pour chaque *Class Identifier* suivants comme décrit ci-dessous :

  ```
  [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\ActiveX Compatibility\
  {XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX}]
  "Compatibility Flags"=dword:00000400
  ```

  Liste des *Class Identifiers* :
  {0002E541-0000-0000-C000-000000000046}
  {0002E559-0000-0000-C000-000000000046}
- utiliser un navigateur alternatif.

6 Solution

Se référer au bulletin de sécurité MS09-043 de Microsoft pour l'obtention des correctifs (cf. section Documentation).

7 Documentation

- Bulletin de sécurité Microsoft 973472 du 13 juillet 2009 :
  http://www.microsoft.com/technet/security/advisory/973472.mspx
- Bulletin de sécurité Microsoft MS09-043 du 11 août 2009 :
  http://www.microsoft.com/france/technet/security/Bulletin/MS09-043.mspx
  http://www.microsoft.com/technet/security/Bulletin/MS09-043.mspx
- Avis CERTA-2009-AVI-331 du 12 août 2009 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2009-AVI-331/
- Référence CVE CVE-2009-1136 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1136

Gestion détaillée du document

13 juillet 2009 version initiale.
12 août 2009 ajout de la solution.