Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 14 août 2007
N° CERTA-2007-AVI-359

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans les Gadgets de Microsoft Windows Vista

Gestion du document

Référence	CERTA-2007-AVI-359
Titre	Vulnérabilités dans les Gadgets de Microsoft Windows Vista
Date de la première version	14 août 2007
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS07-048 du 14 août 2007
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 Windows Vista ;
- Microsoft Windows Vista Édition x64.

3 Résumé

Des vulnérabilités ont été identifiées dans les `gadgets` fournis avec Microsoft Windows Vista. L'exploitation de ces dernières permettrait d'exécuter du code arbitraire à distance sur le système vulnérable.

4 Description

Des vulnérabilités ont été identifiées dans les `gadgets` fournis avec Microsoft Windows Vista. Les `gadgets` sont des applications, ou codes. Ils peuvent se présenter sous forme de contenu HTML qu'il est possible d'afficher

sur le bureau de l'utilisateur. Le contenu HTML dans le gadget est téléchargé depuis un site distant sous forme d'un ensemble de scripts, ensuite exécutés localement.

Les vulnérabilités mentionnées concernent les `gadgets` suivants :

- gadget Météo ;
- gadget Contacts ;
- gadget Titres.

Il est possible, par le biais d'un flux RSS malveillant ou compromis, d'exécuter du code arbitraire à distance sur le système vulnérable.

5 Solution

Se référer au bulletin de sécurité MS07-048 de Microsoft pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Microsoft MS07-048 du 14 août 2007 :
  http://www.microsoft.com/france/technet/security/Bulletin/MS07-048.mspx
  http://www.microsoft.com/technet/security/Bulletin/MS07-048.mspx
- Référence CVE CVE-2007-3032 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3032
- Référence CVE CVE-2007-3033 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3033
- Référence CVE CVE-2007-3891 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3891

Gestion détaillée du document

14 août 2007 version initiale.