Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 13 août 2008
N° CERTA-2008-AVI-405

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans des filtres Microsoft Office

Gestion du document

Référence	CERTA-2008-AVI-405
Titre	Multiples vulnérabilités dans des filtres Microsoft Office
Date de la première version	13 août 2008
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS08-044 du 12 août 2008
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 2000 Service Pack 3 ;
- Microsoft Office XP Service Pack 3 ;
- Microsoft Office 2003 Service Pack 2 ;
- Microsoft Office Project 2002 Service Pack 1 ;
- Pack de conversion Microsoft Office ;
- Microsoft Works 8.

3 Résumé

Des vulnérabilités ont été identifiées dans certains filtres Microsoft Office. L'exploitation de ces dernières peut conduire à l'exécution de code arbitraire à distance par le biais de documents spécialement construits.

4 Description

Des vulnérabilités ont été identifiées dans certains filtres Microsoft Office :

- Office ne manipule pas correctement certains fichiers au format `EPS` ;
- Office ne manipule pas correctement certains fichiers au format `PICT` ayant une valeur incorrecte dans le champ `bits_per_pixel` ;
- Office ne manipule pas correctement certains fichiers au format `BMP` (filtre `BMPIMP32.FLT`) ;
- Office ne manipule pas correctement certains fichiers au format `WPG` (*WordPerfect Graphics*), en particulier via le filtre `WPGIMP32.FLT`.

L'exploitation de ces vulnérabilités peut entraîner l'exécution de code arbitraire à distance suite à une corruption de mémoire.

5 Solution

Se référer au bulletin de sécurité MS08-044 de Microsoft pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Microsoft MS08-044 du 12 août 2008 :
  http://www.microsoft.com/france/technet/security/Bulletin/MS08-044.mspx
  http://www.microsoft.com/technet/security/Bulletin/MS08-044.mspx
- Référence CVE CVE-2008-3018 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3018
- Référence CVE CVE-2008-3019 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3019
- Référence CVE CVE-2008-3020 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3020
- Référence CVE CVE-2008-3021 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3021
- Référence CVE CVE-2008-3460 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3460
- Avis de sécurité TippingPoint ZDI-08-049 du 12 août 2008 :
  http://www.zerodayinitiative.com/advisories/ZDI-08-049
- Avis de sécurité iDefense du 12 août 2008 :
  http://labs.idefense.com/intelligence/vulnerabilities/

Gestion détaillée du document

13 août 2008 version initiale.