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 décembre 2011
N° CERTA-2011-ALE-006-003

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Exploitation d'une vulnérabilité dans la gestion des polices TrueType sur Windows

Gestion du document

Référence	CERTA-2011-ALE-006-003
Titre	Exploitation d'une vulnérabilité dans la gestion des polices TrueType sur Windows
Date de la première version	04 novembre 2011
Date de la dernière version	14 décembre 2011
Source	Avis de sécurité Microsoft 2639658
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

Toutes les versions supportées de Microsoft Windows sont affectées à l'exception des éditions *Core* de Windows Server 2008 et Windows Serveur 2008 R2 qui ne sont pas affectées par cette vulnérabilité.

3 Résumé

Symantec et le *Laboratory of Cryptography and System Security* (CrySys) ont découvert une vulnérabilité non corrigée et exploitée sur l'Internet par le logiciel malveillant Duqu. Microsoft a publié un avis de sécurité 2639658 détaillant les mesures de protection immédiates pouvant être mises en œuvre.

4 Description

Le logiciel malveillant Duqu se propage notamment via l'exploitation d'une vulnérabilité non corrigée dans les polices TrueType. À ce jour, le code malveillant utilise pour vecteur un document Microsoft Word mais toute application reposant sur la fonctionnalité des polices embarquées est potentiellement vulnérable.

Pour mettre en œuvre son code d'exploitation, l'attaquant va intégrer à un document une police malveillante dont le chargement par le système va déclencher l'exécution de code arbitraire.

Enfin, il est important de prendre en compte les différents vecteurs que la plateforme Windows propose en terme de transport de polices de caractères.

La technologie *Embedded Open Type* (EOT) permet d'intégrer des polices TrueType à des documents HTML. Lors de l'ouverture d'une page Web, Internet Explorer va ouvrir le conteneur EOT et déclencher le chargement par Windows de la police TrueType contenue provoquant alors l'exécution de code arbitraire. Internet Explorer est le seul navigateur à supporter la technologie *Embedded Open Type*.

Au moment de la publication de cet avis, seuls des contournements provisoires sont disponibles. Une mise à jour de sécurité serait en cours de développement par Microsoft.

5 Contournement provisoire

Le contournement proposé par Microsoft repose sur le blocage des fonctionnalités de polices embarquées (T2EMBED.DLL).

Les polices embarquées, par exemple dans un document, ne sont alors plus transmises au composant Windows vulnérable en charge des polices TrueType. Le déploiement du contournement implique que les applications utilisant cette technologie connaîtront des problèmes d'affichage et/ou d'impression, les polices embarquées n'étant plus utilisables.

Ce déploiement peut être réalisé par script ou via un paquetage de type *FixIt*.

Ce contournement est aussi déployable par stratégies de groupe.

Le CERTA recommande de tester ce contournement avant tout déploiement à grande échelle (notamment installation, fonctionnalités de base et désinstallation).

6 Solution

Se référer au bulletin de sécurité MS011-087 de l'éditeur pour les détails d'obtention des correctifs (cf. section Documentation).

7 Documentation

- Article de bloc-notes (blog) de Symantec sur l'installateur Duqu :
  http://www.symantec.com/connect/w32-duqu_status-updates_installer-zero-day-exploit
- Avis de sécurité Microsoft 2639658 du 03 novembre 2011 :
  http://technet.microsoft.com/fr-fr/security/advisory/2639658
- Fiche de support technique 2639658 relatif au paquetage *FixIt* :
  http://support.microsoft.com/kb/2639658/fr
- Référence CVE CVE-2011-3402 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3402
- Avis du CERTA CERTA-2011-AVI-684 du 14 décembre 2011 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2011-AVI-684
- Bulletin de sécurité Microsoft MS11-087 du 13 décembre 2011 :
  http://technet.microsoft.com/fr-fr/security/bulletin/MS11-087
  http://technet.microsoft.com/en-us/security/bulletin/MS11-087

Gestion détaillée du document

04 novembre 2011 version initiale.

04 novembre 2011 documentation des vecteurs HTML basés sur la technologie Embedded Open Type.

09 novembre 2011 ajout de la référence CVE.

14 décembre 2011 ajout du correctif Microsoft.