Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 03 août 2010
N° CERTA-2010-ALE-010-002

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Vulnérabilité dans le Shell de Microsoft Windows

Gestion du document

Référence	CERTA-2010-ALE-010-002
Titre	Vulnérabilité dans le Shell de Microsoft Windows
Date de la première version	19 juillet 2010
Date de la dernière version	03 août 2010
Source(s)	Avis de sécurité Microsoft #2286198 du 16 juillet 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.

2 Systèmes affectés

Toutes les versions de Microsoft Windows.

3 Résumé

Une vulnérabilité dans le *shell* `Windows` permet à un utilisateur distant malintentionné d'exécuter du code arbitraire.

4 Description

Une vulnérabilité du *shell* `Windows` existe dans la gestion des fichiers de raccourcis *.lnk* et permet l'exécution à distance de code arbitraire avec les droits de l'utilisateur connecté sur la machine.

Les fichiers *.lnk* permettent de créer des raccourcis vers des fichiers ou des répertoires.

Microsoft a mis à jour son avis pour indiquer que les fichiers *.pif* sont aussi vulnérables.

L'exploitation de la vulnérabilité survient lors de l'ouverture, via l'explorateur `Windows`, d'un dossier contenant les fichiers malformés. La méthode d'infection typique est l'ouverture d'une clé *USB* infectée, l'exploitation fonctionnant même si `Autorun` a été désactivé.

Cependant, les périphériques *USB* ne sont qu'un vecteur d'exploitation, la vulnérabilité peut être aussi exploitée via des partages réseaux, des liens `WebDav`, ou tout autre vecteur menant à l'affichage des fichiers malformés dans l'explorateur de fichier `Windows`.

Cette vulnérabilité est activement exploitée sur l'Internet (voir l'alerter CERTA-2010-ALE-009).

5 Contournement provisoire

Comme documenté dans l'avis Microsoft #2286198, la désactivation de l'affichage des icônes des raccourcis *.lnk* et *.pif* empêche l'exploitation de la vulnérabilité.

Microsoft a publié un *FixIt* permettant de déployer le contournement plus facilement (voir section Documentation).

La procédure manuelle est :

- Faire une copie du contenu de la clé de registre :
  `HKEY_CLASSES_ROOT\lnkfile\shellex\IconHandler` ;
- Puis, editer la valeur «*Par défaut*» de cette clé et en supprimer le contenu ;
- Faire une copie du contenu de la clé de registre :
  `HKEY_CLASSES_ROOT\piffile\shellex\IconHandler` ;
- Puis, editer la valeur «*Par défaut*» de cette clé et en supprimer le contenu ;
- Redémarrer la machine ou `explorer.exe`.

Attention, cette manipulation désactive l'affichage de tous les icônes des raccourcis , y compris ceux du menu *démarrer* de `Windows`.

6 Solution

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

7 Documentation

- Bulletin de sécurité Microsoft MS10-046 du 03 août 2010 :
  http://www.microsoft.com/france/technet/security/Bulletin/MS10-046.mspx
  http://www.microsoft.com/technet/security/Bulletin/MS10-046.mspx
- Avis CERTA-2010-AVI-353 du 3 août 2010 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2010-AVI-353
- Avis de sécurité Microsoft #2286198 du 16 juillet 2010 :
  http://www.microsoft.com/technet/security/advisory/2286198.mspx
- Fixit Microsoft du 21 juillet 2010 :
  http://support.microsoft.com/kb/2286198
- Alerte CERTA-2010-ALE-009 du 16 juillet 2010 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2010-ALE-009
- Référence CVE CVE-2010-2568 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2568

Gestion détaillée du document

19 juillet 2010 version initiale.

21 juillet 2010 ajout de la vulnérabilité des fichiers .lnk, modification de la section Contournement , ajout du FixIt Microsoft.

03 août 2010 ajout de la section Solution et ajout de la référence au bulletin de sécurité Microsoft dans la section Documentation. .