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 novembre 2007
N° CERTA-2007-ALE-015-003

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Vulnérabilité dans le traitement des URI sous Windows

Gestion du document

Référence	CERTA-2007-ALE-015-003
Titre	Vulnérabilité dans le traitement des URI sous Windows
Date de la première version	10 octobre 2007
Date de la dernière version	14 novembre 2007
Source(s)	
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 commandes arbitraires à distance.

2 Systèmes affectés

- Windows XP SP 2 avec *Internet Explorer 7* installé ;
- Windows 2003 Server SP2 avec *Internet Explorer 7* installé.

D'autres versions de Windows peuvent être affectées, le principal prérequis étant la présence d'*Internet Explorer 7*.

3 Résumé

Une vulnérabilité dans la gestion des URI dans Windows permet l'exécution de commandes arbitraires à distance.

4 Description

Une vulnérabilité dans le traitement des URI dans Windows permet l'exécution de commandes à distance. La présence d'*Internet Explorer 7* (IE7) est nécessaire pour l'exploitation de cette vulnérabilité, car la gestion des URI est liée à ce programme. Cette alerte est une extension de l'alerte CERTA-2007-ALE-013, plusieurs applications étant concernées par cette vulnérabilité. Plus précisément, les chaînes de caractères passées en argument de certaines URI ne sont contrôlées ni par IE7 qui en assure le traitement, ni par un certain nombre d'applications (comme *Acrobat Reader*, *Miranda*, etc.) qui appellent la fonction vulnérable de Windows.

Il n'existe pour le moment aucun contournement provisoire pour ce problème qui n'ait de conséquences lourdes pour le fonctionnement du système et des applications. Il est toutefois possible que des éditeurs proposent des correctifs ou des contournements pour leur application, comme ce fut le cas pour *Mozilla Firefox* (voir alerte CERTA-2007-ALE-013) ou *Adobe Reader* (voir Documentation).

Mise à jour du 11 octobre 2007 :
Microsoft vient de publier l'avis de sécurité 943521 confirmant le problème.

Mise à jour du 24 octobre 2007 :
Adobe publie un correctif pour la version 8.1 des produits vulnérables.

Mise à jour du 14 novembre 2007 :
Microsoft publie un correctif décrit dans son bulletin MS07-061. Ce dernier est présenté dans l'avis CERTA-2007-AVI-489.

5 Contournements provisoires

Les contournements ne sont pas simples, comme il a été mentionné dans la section ci-dessus. Néanmoins, quelques mesures peuvent être entreprises pour limiter les risques :

- des règles de filtrage concernant des liens suspects peuvent être mises en place au niveau des passerelles Web ou de messagerie qui inspectent le contenu. Par exemple, le champ `mailto:` ne doit pas être *a priori* suivi d'une chaîne de caractère contenant `../..` ou `%`, mais d'une adresse électronique valide. Des règles peuvent également être précisées pour les champs de type : `http:`, etc. De manière générale, tout type de liens qui n'est pas attendu ou explicitement autorisé doit être filtré.
- les fichiers aux formats PDF peuvent être convertis dans d'autres formats (HTML, PS, TXT) ;
- des clés de registre peuvent être modifiées au niveau des postes clients pour l'interprétation des champs protocolaires. Cette solution a été abordée dans une alerte publiée par Adobe. Elle est cependant assez radicale, et peut provoquer plusieurs dysfonctionnements.

6 Solution

Appliquer les correctifs décrits dans le bulletin de sécurité MS07-061 de Microsoft publié le 13 novembre 2007.

7 Documentation

- Avis CERTA-2007-AVI-489 du 14 novembre 2007 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2007-AVI-489/
- Bulletin de sécurité Microsoft MS07-061 du 13 novembre 2007 :
  http://www.microsoft.com/france/technet/security/Bulletin/MS07-061.mspx
  http://www.microsoft.com/technet/security/Bulletin/MS07-061.mspx
- Alerte CERTA-2007-ALE-013 du 31 juillet 2007 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-013/index.html
- Document du CERTA CERTA-2007-AVI-455 du 24 octobre 2007 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2007-AVI-455/index.html
- Bulletin de sécurité Adobe du 05 octobre 2007 :
  http://www.adobe.com/support/security/advisories/apsa07-04.html
- Bulletin de sécurité Adobe ASPB07-18 du 22 octobre 2007 :
  http://www.adobe.com/support/security/bulletins/ASPB07-18.html

- Avis de sécurité Microsoft 943521 du 10 octobre 2007 :
  http://www.microsoft.com/technet/security/advisory/943521.mspx
- Commentaires de Microsoft aux développeurs concernant la gestion des manipulateurs de protocoles :
  http://blogs.msdn.com/ie/archive/2007/07/18/enriching-the-web-safely-how-to-create-application-protocol-handlers.aspx
- Référence CVE CVE-2007-3896 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3896
- Référence CVE CVE-2007-5020 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5020

Gestion détaillée du document

10 octobre 2007 version initiale.

11 octobre 2007 ajout de l'avis 943521 de Microsoft et de la référence CVE associée.

24 octobre 2007 ajout de l'avis ASPB07-18 d'Adobe et de la référence CVE associée.

14 novembre 2007 ajout de la référence au bulletin MS07-061 de Microsoft.