

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Débordement de mémoire dans Microsoft Commerce Server 2000 et 2002

Conditions d'utilisation de ce document : <http://www.certa.ssi.gouv.fr/certa/apropos.html>
Dernière version de ce document : <http://www.certa.ssi.gouv.fr/site/CERTA-2002-AVI-135>

Gestion du document

Référence	CERTA-2002-AVI-135
Titre	Débordement de mémoire dans Microsoft Commerce Server 2000 et 2002
Date de la première version	27 juin 2002
Date de la dernière version	–
Source(s)	Bulletin de sécurité MS02-033 de Microsoft
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 ;
- déni de service ;
- élévation de privilèges.

2 Systèmes affectés

Microsoft Commerce Server 2000 et 2002.

3 Résumé

Il existe de multiples vulnérabilités dans Microsoft Commerce Server 2000 et 2002.

4 Description

Microsoft Commerce Server 2000 et 2002 sont des serveurs web permettant le commerce en ligne.

Quatre vulnérabilités présentes dans Microsoft Commerce Server ont été récemment révélées. Les 3 premières vulnérabilités concernent *Profile Service* et OWC qui sont des composants de Commerce Server 2000 uniquement.

- *Profile Service* est un service permettant à un utilisateur authentifié d'administrer à distance son propre profil sur Commerce Server 2000.
Sous Commerce Server 2000, un débordement de mémoire dans une fonction de *Profile Service* manipulant des appels d'API (*Application Programming Interface*) permet à un utilisateur mal intentionné authentifié d'exécuter du code arbitraire dans le contexte de sécurité de l'utilisateur *LocalSystem* ou bien de stopper le programme Commerce Server 2000 à distance.
Profile Service est installé mais n'est pas activé par défaut. Pour que cette vulnérabilité soit exploitable, il faut que l'administrateur de Commerce Server 2000 ait activé *Profile Service*.
- *Office Web Components* (OWC) est un ensemble d'outils d'administration à distance pour Commerce Server. Il est installé par défaut avec Commerce Server 2000 et n'affecte que ce dernier.
Sous Commerce Server 2000, un utilisateur mal intentionné connecté localement peut, en fournissant des données malformées au gestionnaire d'installation de OWC, exécuter du code arbitraire dans le contexte de sécurité de l'utilisateur *LocalSystem* ou bien arrêter le programme Commerce Server.
- Un autre débordement de mémoire de l'outil de gestion d'installation de OWC permet à un utilisateur mal intentionné connecté localement d'exécuter du code arbitraire avec ses propres permissions.
Nota : Dans le cadre des deux vulnérabilités OWC, il est à noter qu'un utilisateur sans privilèges ne devrait pas avoir un accès local au serveur.
- Les filtres ISAPI sont des programmes qui répondent à des requêtes HTTP reçues par le serveur web. Microsoft Commerce Server installe une bibliothèque dynamique (DLL) Windows avec le filtre ISAPI *AuthFilter* qui permet l'utilisation de différentes méthodes d'authentification.
Une variante de la vulnérabilité des filtres ISAPI décrite dans le bulletin de sécurité CERTA-2002-AVI-044 permet à un utilisateur mal intentionné de prendre le contrôle total sur le serveur au moyen d'un débordement de mémoire du filtre *AuthFilter* de Commerce Server 2000 et 2002.
Les filtres ISAPI sont installés sur Internet Information Server, mais le filtre *AuthFilter* n'est présent que sur Commerce Server, les serveurs web IIS ne sont donc pas affectés par cette vulnérabilité.

5 Contournement provisoire

Le gestionnaire d'installation de OWC n'est plus nécessaire après l'installation de celui-ci. Et le correctif ne fait que diminuer les risques d'exploitation de ces vulnérabilités.

Pour plus de sécurité, Microsoft recommande de supprimer l'exécutable `boowc.exe` situé dans le répertoire `Program files\Microsoft Commerce Server\widgets\owc` de votre système.

6 Solution

Se référer au bulletin de sécurité Microsoft MS02-033 (Voir paragraphe Documentation) pour connaître la disponibilité des correctifs pour Commerce Server 2000 et 2002.

7 Documentation

Bulletin de sécurité MS02-033 de Microsoft :
<http://www.microsoft.com/technet/security/bulletin/MS02-033.asp>
Avis du CERTA : CERTA-2002-AVI-044.

Gestion détaillée du document

27 juin 2002 version initiale.